

# **Document made available under the Patent Cooperation Treaty (PCT)**

International application number: PCT/JP2005/022788

International filing date: 12 December 2005 (12.12.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-360436  
Filing date: 13 December 2004 (13.12.2004)

Date of receipt at the International Bureau: 30 January 2006 (30.01.2006)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2004年12月13日

出願番号 Application Number: 特願2004-360436

パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is

出願人 Applicant(s): 松下電器産業株式会社  
国立大学法人 東京大学

2006年 1月11日

特許庁長官  
Commissioner,  
Japan Patent Office

中嶋誠記

【書類名】 特許願  
【整理番号】 2048160371  
【提出日】 平成16年12月13日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G09C 1/00  
【発明者】  
　【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
　【氏名】 野仲 真佐男  
【発明者】  
　【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
　【氏名】 中野 稔久  
【発明者】  
　【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
　【氏名】 布田 裕一  
【発明者】  
　【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
　【氏名】 大森 基司  
【発明者】  
　【住所又は居所】 東京都文京区本郷7-3-1 国立大学法人東京大学内  
　【氏名】 五味 剛  
【発明者】  
　【住所又は居所】 東京都文京区本郷7-3-1 国立大学法人東京大学内  
　【氏名】 古原 和邦  
【発明者】  
　【住所又は居所】 東京都文京区本郷7-3-1 国立大学法人東京大学内  
　【氏名】 今井 秀樹  
【特許出願人】  
　【識別番号】 000005821  
　【氏名又は名称】 松下電器産業株式会社  
【特許出願人】  
　【識別番号】 504137912  
　【氏名又は名称】 国立大学法人東京大学  
【代理人】  
　【識別番号】 100090446  
　【弁理士】 中島 司朗  
【手数料の表示】  
　【予納台帳番号】 014823  
　【納付金額】 8,000円  
【その他】 国等以外のすべての者の持分の割合 1/2  
【提出物件の目録】  
　【物件名】 特許請求の範囲 1  
　【物件名】 明細書 1  
　【物件名】 図面 1  
　【物件名】 要約書 1  
　【包括委任状番号】 9003742

## 【書類名】特許請求の範囲

### 【請求項 1】

利用者端末のクローンを発見するクローン端末発見システムであって、

前記クローン端末発見システムは、前記利用者端末にクローンが存在するか否かを判断する管理センタと、前記利用者端末に関する利用者端末端末情報を前記管理センタへ供給する一以上の情報収集サーバと、前記利用者端末端末情報を前記情報収集サーバへ供給する一以上の前記利用者端末と、から構成され、前記管理センタと前記情報収集サーバは通信路を介して通信可能であって、

前記管理センタは、

管理センタ端末情報を保持する管理センタ記録手段と、

前記情報収集サーバから前記利用者端末端末情報を取得する手段と、

前記管理センタ端末情報及び前記利用者端末端末情報を基に、前記利用者端末にクローンが存在するか否か判断する端末情報確認手段と、

前記端末情報確認手段において、前記利用者端末にクローンが存在するか否かの判断結果を外部へ報知する出力手段と、備え、

前記情報収集サーバは、

可搬媒体を介して、前記利用者端末から前記利用者端末端末情報を収集する情報収集サーバ可搬媒体挿入処理手段と、

通信路を介して、前記前記利用者端末端末情報を前記管理センタへ供給する情報収集サーバ送信処理手段と、を備え、

前記利用者端末は、

前記利用者端末固有の前記利用者端末端末情報を保持する利用者端末記録手段と、

前記可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給する可搬媒体データ書き込み手段と、

を備えることを特徴とする、クローン端末発見システム。

### 【請求項 2】

前記管理センタは、さらに、

前記利用者端末端末情報とは異なる前記第二利用者端末端末情報を生成する端末情報生成手段と、

前記通信路を介して、前記第二利用者端末端末情報を前記情報収集サーバへ供給する管理センタ送信手段、とを備え、

前記情報収集サーバは、さらに、

前記通信路を介して、前記管理センタから前記第二利用者端末端末情報を取得する情報収集サーバ受信手段と、

前記可搬媒体を介して、前記第二利用者端末端末情報を前記利用者端末へ供給する可搬媒体データ書き込み手段と、を備え、

前記利用者端末は、さらに、

前記可搬媒体を介して、前記第二利用者端末端末情報を前記情報収集サーバから取得する

利用者端末可搬媒体挿入処理手段と、

前記第二利用者端末端末情報を基に、前記利用者端末端末情報を更新する端末情報更新手段と、を備えることを特徴とする、請求項 1 記載のクローン端末発見システム。

### 【請求項 3】

前記端末情報生成手段は、前記情報収集サーバから前記利用者端末端末情報を取得する毎に、前記第二利用者端末端末情報を生成すること、

を特徴とする請求項 2 記載のクローン端末発見システム。

### 【請求項 4】

前記端末情報生成手段は、前記情報収集サーバから前記利用者端末端末情報を取得した回数が予め与えられる数を超えた場合、もしくは、予め指定される期間中に 1 回のみ、前記第二利用者端末端末情報を生成すること、

を特徴とする請求項 2 記載のクローン端末発見システム。

#### 【請求項 5】

前記利用者端末端末情報、及び、前記管理センタ端末情報、及び、前記第二利用者端末端末情報のそれぞれは、前記利用者端末を一意に特定する利用者端末識別子と前記管理センタが生成した乱数を含み、

前記端末情報生成手段で作成される前記第二利用者端末端末情報は、前記利用者端末端末情報に含まれる前記利用者端末識別子と同じ前記利用者端末識別子を含み、前記利用者端末端末情報に含まれる前記乱数とは異なる乱数を含むこと、

を特徴とする請求項 2 から請求項 4 に記載のクローン端末発見システム。

#### 【請求項 6】

前記端末情報確認手段は、前記管理センタ端末情報に含まれる乱数と前記利用者端末端末情報に含まれる乱数が異なる場合に、前記利用者端末にクローンが存在すると判断することを、

を特徴とする請求項 5 に記載のクローン端末発見システム。

#### 【請求項 7】

前記管理センタ記録手段は、さらに、一以上のタイトル鍵を保持し、

前記管理センタ送信手段は、さらに、何れかの前記タイトル鍵を前記情報収集サーバへ供給し、

前記情報収集サーバ受信手段は、さらに、前記管理センタから前記タイトル鍵を取得し、

前記可搬媒体データ書込手段は、さらに、前記タイトル鍵を前記利用者端末へ供給し、前記利用者端末可搬媒体挿入処理手段は、さらに、前記タイトル鍵を前記情報収集サーバから取得し、

前記利用者端末は、さらに、

前記タイトル鍵を基にコンテンツが暗号化された暗号化コンテンツを保持する手段と、

前記タイトル鍵を基に、前記暗号化コンテンツを復号化して、前記コンテンツを取得するデスクランブル処理手段と、

前記コンテンツを逐次外部へ出力する出力手段と、

を備えることを特徴とする、請求項 2 から請求項 6 に記載のクローン端末発見システム。

#### 【請求項 8】

前記管理センタ記録手段は、さらに、前記利用者端末と予め共有している前記利用者端末固有の個別鍵と、一以上のタイトル鍵を保持し、

前記管理センタは、さらに、

前記個別鍵を基に前記タイトル鍵を暗号化し、暗号化タイトル鍵を生成する暗号化タイトル鍵生成手段と、を備え、

前記管理センタ送信手段は、さらに、前記暗号化タイトル鍵を前記情報収集サーバへ供給し、

前記情報収集サーバ受信手段は、さらに、前記管理センタから前記暗号化タイトル鍵を取得し、

前記可搬媒体データ書込手段は、さらに、前記暗号化タイトル鍵を前記利用者端末へ供給し、

前記利用者端末可搬媒体挿入処理手段は、さらに、前記暗号化タイトル鍵を前記情報収集サーバから取得し、

前記利用者端末記録手段は、さらに、前記個別鍵を保持し、

前記利用者端末は、さらに、

前記タイトル鍵を基にコンテンツが暗号化された暗号化コンテンツを保持する手段と、

前記個別鍵を基に前記暗号化タイトル鍵の復号化を行い、前記タイトル鍵を取得する

暗号化タイトル鍵復号化手段と、

前記タイトル鍵を基に、前記暗号化コンテンツを復号化して、前記コンテンツを取得するデスクランブル処理手段と、

前記コンテンツを逐次外部へ出力する出力手段と、

を備えることを特徴とする請求項 2 から請求項 6 に記載のクローン端末発見システム。

#### 【請求項 9】

第一可搬媒体に前記暗号化コンテンツが記録されており、

前記利用者端末は、さらに、

前記第一可搬媒体から前記暗号化コンテンツを取得する第一可搬媒体アクセス手段と

、  
を備えることを特徴とする請求項 7 から請求項 8 に記載のクローン端末発見システム。

#### 【請求項 10】

利用者端末にクローンが存在するか否か判断する管理センタであって、

前記管理センタは、前記利用者端末に関する利用者端末端末情報を前記管理センタへ供給する一以上の情報収集サーバと通信路を介して通信可能であって、前記収集サーバと前記利用者端末は、可搬媒体を介して通信可能であって、

前記管理センタは、

管理センタ端末情報を保持する管理センタ記録手段と、

前記情報収集サーバから前記利用者端末端末情報を取得する手段と、

前記管理センタ端末情報及び前記利用者端末端末情報を基に、前記利用者端末にクローンが存在するか否か判断する端末情報確認手段と、

前記端末情報確認手段において、前記利用者端末にクローンが存在するか否かの判断結果を外部へ報知する出力手段と、

を備えることを特徴とする、管理センタ。

#### 【請求項 11】

前記管理センタは、さらに、

前記利用者端末端末情報とは異なる前記第二利用者端末端末情報を生成する端末情報生成手段と、

前記通信路を介して、前記第二利用者端末端末情報を前記情報収集サーバへ供給する管理センタ送信手段と、

を備えることを特徴とする、請求項 10 記載の管理センタ。

#### 【請求項 12】

前記端末情報生成手段は、前記情報収集サーバから前記利用者端末端末情報を取得する毎に、前記第二利用者端末端末情報を生成すること、

を特徴とする請求項 11 記載の管理センタ。

#### 【請求項 13】

前記端末情報生成手段は、前記情報収集サーバから前記利用者端末端末情報を取得した回数が予め与えられる数を超えた場合、もしくは、予め与えられる期間中に 1 回のみ、前記第二利用者端末端末情報を生成すること、

を特徴とする請求項 11 記載の管理センタ。

#### 【請求項 14】

前記利用者端末端末情報、及び、前記管理センタ端末情報、及び、前記第二利用者端末端末情報のそれぞれは、前記利用者端末を一意に識別可能な利用者端末識別子と前記管理センタが生成した乱数を含み、

前記端末情報生成手段で作成される前記第二利用者端末端末情報は、前記利用者端末端末情報に含まれる前記利用者端末識別子と同じ前記利用者端末識別子を含み、前記利用者端末端末情報に含まれる前記乱数とは異なる乱数を含むこと、

を特徴とする請求項 11 から請求項 13 に記載の管理センタ。

#### 【請求項 15】

前記端末情報確認手段は、前記管理センタ端末情報に含まれる乱数と前記利用者端末端

末情報に含まれる乱数が異なる場合に、前記利用者端末にクローンが存在すると判断すること、

を特徴とする請求項 1 4 に記載の管理センタ。

#### 【請求項 1 6】

前記管理センタ記録手段は、さらに、一以上のタイトル鍵を保持し、

前記管理センタ送信手段は、さらに、何れかの前記タイトル鍵を前記情報収集サーバへ供給すること、

を特徴とする請求項 1 1 から請求項 1 5 に記載の管理センタ。

#### 【請求項 1 7】

前記管理センタ記録手段は、さらに、前記利用者端末と予め共有している一以上の前記利用者端末固有の個別鍵と、一以上のタイトル鍵を保持し、

前記管理センタは、さらに、

前記個別鍵を基に前記タイトル鍵を暗号化し、暗号化タイトル鍵を生成する暗号化タイトル鍵生成手段と、を備え、

前記管理センタ送信手段は、さらに、前記暗号化タイトル鍵を前記情報収集サーバへ供給すること、

を特徴とする請求項 1 1 から請求項 1 6 に記載の管理センタ。

#### 【請求項 1 8】

利用者端末に関する利用者端末端末情報を管理センタへ供給する情報収集サーバであって、

前記情報収集サーバは、前記利用者端末にクローンが存在するか否か判断する管理センタと通信路を介して通信可能であって、さらに、前記利用者端末と可搬媒体を介して通信可能であって、

前記情報収集サーバは、

前記可搬媒体を介して、前記利用者端末から前記利用者端末端末情報を収集する情報収集サーバ可搬媒体挿入処理手段と、

前記通信路を介して、前記前記利用者端末端末情報を前記管理センタへ供給する情報収集サーバ送信処理手段と、

を備えることを特徴とする、情報収集サーバ。

#### 【請求項 1 9】

利用者端末固有の利用者端末端末情報を情報収集サーバへ供給する利用者端末であって、

前記利用者端末は、前記利用者端末端末情報を前記管理センタへ供給する一以上の情報収集サーバと可搬媒体を介して通信可能であって、さらに、前記利用者端末にクローンが存在するか否か判断する管理センタと前記情報収集サーバは通信路を介して通信可能であって、

前記利用者端末は、

前記利用者端末端末情報を保持する利用者端末記録手段と、

前記可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給する可搬媒体データ書込手段と、

を備えることを特徴とする、利用者端末。

#### 【請求項 2 0】

前記利用者端末は、さらに、

前記可搬媒体を介して、前記第二利用者端末端末情報を前記情報収集サーバから取得する利用者端末可搬媒体挿入処理手段と、

前記第二利用者端末端末情報を基に、保持する前記利用者端末端末情報を更新する端末情報更新手段と

、を備えることを特徴とする、請求項 1 9 記載の利用者端末。

#### 【請求項 2 1】

前記利用者端末可搬媒体挿入処理手段は、さらに、前記タイトル鍵を前記情報収集サー

バから取得し、

前記利用者端末は、さらに、

前記タイトル鍵を基にコンテンツが暗号化された暗号化コンテンツを保持する手段と、

前記タイトル鍵を基に前記暗号化コンテンツを復号化して、前記コンテンツを取得するデスクランブル処理手段と、

前記コンテンツを逐次外部へ出力する出力手段と、

を備えることを特徴とする、請求項19から請求項20に記載の利用者端末。

#### 【請求項22】

前記利用者端末可搬媒体挿入処理手段は、さらに、前記暗号化タイトル鍵を前記情報収集サーバから取得し、

前記利用者端末記録手段は、さらに、前記利用者端末固有の個別鍵を保持し、  
前記利用者端末は、さらに、

前記タイトル鍵を基にコンテンツが暗号化された暗号化コンテンツを保持する手段と、

前記個別鍵を基に前記暗号化タイトル鍵の復号化を行い、前記タイトル鍵を取得する暗号化タイトル鍵復号化手段と、

前記タイトル鍵を基に前記暗号化コンテンツを復号化して、前記コンテンツを取得するデスクランブル処理手段と、

前記コンテンツを逐次外部へ出力する出力手段と、

を備えることを特徴とする、請求項19から請求項20に記載の利用者端末。

#### 【請求項23】

第一可搬媒体に前記暗号化コンテンツが記録されており、

前記利用者端末は、さらに、

前記第一可搬媒体から前記暗号化コンテンツを取得する第一可搬媒体アクセス手段と、

を備えることを特徴とする、請求項21から請求項22に記載の利用者端末。

#### 【請求項24】

利用者端末のクローンが存在するか否かを判断することを目的に、利用者端末端末情報を情報収集サーバへ供給する情報供給方法であって、

前記情報収集方法は、

固有の前記利用者端末端末情報を保持するステップと、

可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給するステップと、

を備えることを特徴とする、情報供給方法。

#### 【請求項25】

前記情報供給方法は、さらに、

前記可搬媒体を介して、前記第二利用者端末端末情報を前記情報収集サーバから取得するステップと、

前記第二利用者端末端末情報を基に、保持する前記利用者端末端末情報を更新するステップと、

を備えることを特徴とする、請求項24記載の情報供給方法。

#### 【請求項26】

利用者プログラムのクローンが存在するか否かを判断することを目的に、利用者端末端末情報を情報収集サーバへ供給する利用者プログラムであって、

前記利用者プログラムは、前記利用者プログラムに関する利用者プログラム情報を前記管理センタへ供給する一以上の情報収集サーバと可搬媒体を介して通信可能であって、前記利用者プログラムにクローンが存在するか否か判断する管理センタと前記情報収集サーバは通信路を介して通信可能であって、

前記利用者プログラムは、

前記利用者プログラム固有の前記利用者プログラム情報を保持するステップと、  
前記可搬媒体を介して、前記利用者プログラム情報を前記情報収集サーバへ供給する  
ステップと、  
を備えることを特徴とする、利用者プログラム。

【請求項 27】

前記利用者プログラムは、さらに、  
前記可搬媒体を介して、前記第二利用者プログラム情報を前記情報収集サーバから取  
得するステップと、  
前記第二利用者プログラム情報を基に、保持する前記利用者プログラム情報を更新す  
るステップと、  
を備えることを特徴とする、請求項 26 記載の利用者プログラム。

【請求項 28】

請求項 26 に記載のプログラムを記録した媒体。

【請求項 29】

請求項 27 に記載のプログラムを記録した媒体。

【請求項 30】

利用者端末のクローンが存在するか否かを判断することを目的に、利用者端末端末情報  
を情報収集サーバへ供給する利用者端末の集積回路であって、

前記利用者端末は、前記利用者端末端末情報を前記管理センタへ供給する一以上の情報  
収集サーバと可搬媒体を介して通信可能であって、さらに、前記利用者端末にクローンが  
存在するか否か判断する管理センタと前記情報収集サーバは通信路を介して通信可能であ  
って、

前記集積回路は、

前記利用者端末固有の前記利用者端末端末情報を保持する利用者端末記録手段を備え  
、

前記利用者端末は、

前記可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給する可  
搬媒体データ書込手段と、

を備えることを特徴とする、集積回路。

【書類名】明細書

【発明の名称】クローン端末発見方法

【技術分野】

【0001】

本発明は、映画や音楽などの著作物であるコンテンツのデジタル化データを再生するシステムに関し、特にクローン端末を利用したコンテンツの再生による著作権侵害を防止するために、クローン端末を発見、あるいは特定するクローン端末発見システムに関する。

【背景技術】

【0002】

近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からなるデジタルコンテンツ（以下、コンテンツ）を生成して、光ディスク等の大容量記録媒体に格納して配布する、あるいはネットワークや放送を介して配信するシステムが登場している。

一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピーといった不正利用を防止するために暗号化技術が用いられる。

【0003】

具体的には、コンテンツのある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号化鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号して、コンテンツの再生等を行うことができる、というものである。なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化して記録する方法や、コンテンツのある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等がある。

【0004】

このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析において、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する記録装置、再生装置、あるいはソフトウェアを作成して、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにならざるを得ない。これを鍵無効化技術と呼び、鍵無効化を実現するシステムとして、特許文献1、あるいは特許文献2が開示されている。

【特許文献1】特開2000-31922号公報

【特許文献2】特開2002-281013号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

しかしながら、前記鍵無効化技術が開示されている特許文献においては、外部に漏れた鍵（無効化すべき鍵）を特定する方法については開示されておらず、特定するためには、市場に大量流通したクローン端末／不正ソフトウェアを回収して、内部を解析することでしか特定できないという課題を有していた。

本発明は、前記課題を解決するもので、可搬媒体を利用して、効率的に無効化すべき鍵を発見、あるいは特定することが可能なクローン端末発見システムを提供することを目的とする。

【課題を解決するための手段】

【0006】

前記従来の課題を解決するために、本発明のクローン端末発見システムは、利用者端末のクローンを発見するクローン端末発見システムであって、利用者端末にクローンが存在するか否かを判断する管理センタと、利用者端末に関する利用者端末端末情報を管理センタへ供給する一以上の情報収集サーバと、利用者端末端末情報を情報収集サーバへ供給す

る一以上の前記利用者端末と、から構成され、管理センタと情報収集サーバは通信路を介して通信可能であって、管理センタは、管理センタ端末情報を保持する管理センタ記録手段と、情報収集サーバから利用者端末端末情報を取得する手段と、管理センタ端末情報及び利用者端末端末情報を基に、利用者端末にクローンが存在するか否か判断する端末情報確認手段と、端末情報確認手段において、利用者端末にクローンが存在するか否かの判断結果を外部へ報知する出力手段と、備え、情報収集サーバは、可搬媒体を介して、利用者端末から利用者端末端末情報を収集する情報収集サーバ可搬媒体挿入処理手段と、通信路を介して、利用者端末端末情報を管理センタへ供給する情報収集サーバ送信処理手段と、を備え、利用者端末は、利用者端末固有の利用者端末端末情報を保持する利用者端末記録手段と、可搬媒体を介して、利用者端末端末情報を情報収集サーバへ供給する可搬媒体データ書込手段とを有し、効率的に無効化すべき鍵を発見することができる。

#### 【発明の効果】

##### 【0007】

本発明によれば、効率的に無効化すべき鍵を発見、あるいは特定することが可能である。

#### 【発明を実施するための最良の形態】

##### 【0008】

以下本発明に係るクローン端末発見システムの実施の形態について、図面を参照しながら説明する。

##### (実施の形態1)

本発明に係る第1の実施の形態としてのクローン端末発見システム1について説明する。最初に、図1を用いて本実施形態の概要を説明する。

##### 【0009】

クローン端末発見システム1は、通信路1と管理センタ2と一以上の情報収集サーバ3と一以上の第一可搬媒体4と複数の第二可搬媒体5a～5mと複数の利用者端末6a～6nとから構成される。なお、図1では、情報収集サーバ3と第一可搬媒体4と第二可搬媒体5aと利用者端末6aを一つずつのみ示している。通信路1は、管理センタ2と情報収集サーバ3とが接続されている通信路であり、インターネット等のネットワークである。管理センタ2は、一以上の情報収集サーバ3から第二可搬媒体5a～5mの何れかを介して利用者端末6a～6nの何れかに関する端末情報を受け取り、利用者端末6a～6nにクローンが存在するか否か判断する。ここでクローンの定義は、利用者端末毎に個別に与えられている個別鍵を二台以上の利用者端末が保持している状態であるとする。情報収集サーバ3は、例えば動画コンテンツが記録された光ディスクを販売する小売店に設置され、第二可搬媒体5a～5mに記録されているデータの読み書きが可能な端末であり、第二可搬媒体5a～5mのいずれかが挿入された場合に、以前その第二可搬媒体が挿入されたことのある利用者端末に関する端末情報を管理センタ2へ送信する。第一可搬媒体4は、例えば動画コンテンツが記録されている光ディスク（例えばDVD-ROM）である。第二可搬媒体5a～5mはそれぞれ、データの書き換えが可能なポータブルメディア（例えばSDカード）である。利用者端末6a～6nはそれぞれ、第一可搬媒体4に記録されているデータの読み取り、及び第二可搬媒体5a～5mに記録されているデータの読み書きが可能な端末であり、第一可搬媒体4に記録されているコンテンツを外部へ出力する。ここで、管理センタ2と利用者端末6a～6nの全ての組には、予め各組が共有している利用者端末識別子と個別鍵と乱数が与えられているとし、例えば管理センタ2と利用者端末6aは利用者端末識別子T M I D aと個別鍵I K aと乱数（管理センタ2が保持する乱数を第一管理センタ乱数C R N D 1 aとし、利用者端末6aが保持する乱数を第一利用者端末乱数T M R N D 1 aと呼ぶ）を、管理センタ2と利用者端末6bは利用者端末識別子T M I D bと個別鍵I K bと乱数（管理センタ2が保持する乱数を第一管理センタ乱数C R N D 1 bとし、利用者端末6bが保持する乱数を第一利用者端末乱数T M R N D 1 bと呼ぶ）を、・・・、管理センタ11と利用者端末6nは利用者端末識別子T M I D nと個別鍵I K nと乱数（管理センタ2が保持する乱数を第一管理センタ乱数C R N D nとし、

利用者端末 6 n が保持する乱数を第一利用者端末乱数 TMRNDn と呼ぶ) を予め共有しているとする。

#### 【0010】

ここでは、管理センタ2と情報収集サーバ3と利用者端末6a～6nの動作について、具体例を交えてもう少し詳細に説明する。一例として、利用者端末6aを保有するユーザが、動画コンテンツの入ったある光ディスクを小売店で購入して、利用者端末6aで再生するまでの動作について説明する。ここでは、そのユーザは第二可搬媒体5aを保持しているとする。

#### 【0011】

まず事前設定として、ユーザは第二可搬媒体5aを利用者端末6aへ挿入し、その際利用者端末6aは端末情報として、利用者端末識別子TMI Daと現在保持している第一利用者端末乱数TMRND1aを第二可搬媒体5aへ記録する。

そして、ユーザは小売店へ移動し、コンテンツの記録された第一可搬媒体4(光ディスク)を購入する。その第一可搬媒体4には、コンテンツがコンテンツタイトルに対応するタイトル鍵TLKで暗号化されて記録されているとする。その後、ユーザは小売店に設置されている情報収集サーバ3に可搬媒体5aを挿入し、ユーザ(もしくは店員)は第一可搬媒体4に記録されているコンテンツのタイトルを識別するタイトル識別子TLIDを入力する。そして、情報収集サーバ3は、第二可搬媒体5aに記録されている端末情報である利用者端末識別子TMI Daと第一利用者端末乱数TMRND1aを取得し、入力されたタイトル識別子TLIDと共に管理センタ2へ送信する。端末情報である利用者端末識別子TMI Daと第一利用者端末乱数TMRND1aと、タイトル識別子TLIDを受け取った管理センタ2は、まず管理センタの保持する利用者端末識別子TMI Daに対応する第一管理センタ乱数CRND1aを受け取った第一利用者端末乱数TMRND1aが一致するか確認する。ここで値が一致しない場合、利用者端末識別子TMI Daに対応する利用者端末6aがクローンである旨、外部に出力する。値が一致した場合、まず利用者端末識別子TMI Daに対応する個別鍵IKaを基に、タイトル識別子TLIDに対応するタイトル鍵TLKを暗号化して、暗号化タイトル鍵ENCTLKを生成する。次に、新たに乱数を一つ生成して、その乱数を第二管理センタ乱数CRND2aと第二利用者端末乱数TMRND2aとする。つまり、第二管理センタ乱数CRND2aと第二利用者端末乱数TMRND2aは同じ値となる。そして、情報収集サーバ3へ暗号化タイトル鍵TLKと第二利用者端末乱数TMRND2aを送付し、第二管理センタ乱数CRND2aを格納する。管理センタ2から暗号化タイトル鍵ENCTLKと第二利用者端末乱数TMRND2aを受け取った情報収集サーバ3は、暗号化タイトル鍵TLKと第二利用者端末乱数TMRND2aを第二可搬媒体5aに記録する。

#### 【0012】

第一可搬媒体を小売店で購入したユーザは、まず利用者端末6aへ第二可搬媒体5aを挿入する。利用者端末6aは、第二可搬媒体5aから暗号化タイトル鍵TLKと第二利用者端末乱数TMRND2aを受け取る。まず、暗号化タイトル鍵ENCTLKを自身の保持する個別鍵IKaを基に復号化し、タイトル鍵TLKを取得し、利用者端末6a内に格納する。次に、利用者端末6aが保持する第一利用者端末乱数TMRND1aの値を第二利用者端末乱数TMRND2aの値に入れ替える。その後、利用者端末6aに第一可搬媒体4を挿入し、挿入された第一可搬媒体4に記録されたコンテンツタイトルに対応するタイトル鍵TLKを基に、記録されている暗号化コンテンツENCNTを復号化してコンテンツCNTを取得し、外部へ出力する。

#### 【0013】

なお、ここで用いる暗号処理は、秘密鍵暗号方式による暗号処理である。秘密鍵暗号方式による暗号処理の一例は、ブロック暗号AESである。AESについては、公知であるので説明を省略する。

以上が、本実施形態の概要である。以下に、本発明のクローン端末発見システムの一実施形態であるクローン端末発見システム1の詳細について説明を行う。これらの構成要素

について詳細に説明する。

#### 【0014】

##### <クローン端末発見システム1の構成>

クローン端末発見システム1は、通信路1と管理センタ2と一以上の情報収集サーバ3と一以上の第一可搬媒体4と複数の第二可搬媒体5a～5mと複数の利用者端末6a～6nとから構成される。以下に、これらの構成要素について詳細に説明する。まず、通信路1及び第一可搬媒体4及び第二可搬媒体5a～5mについて述べ、続いて管理センタ2及び情報収集サーバ3及び利用者端末6a～6nの構成と動作について図を用いて説明する。なお、第二可搬媒体5a～5mのそれぞれは同じ構成であるので、第二可搬媒体5aを例に挙げて説明する。また、利用者端末6a～6nのそれぞれはほぼ同じ構成であるので、はじめに利用者端末6aを例に挙げて説明し、最後に各利用者端末6a～6nの違いについて説明する。

#### 【0015】

##### <通信路1の構成>

通信路は、例えば、インターネット、電話回線や専用線等のようなネットワークである。

##### <第一可搬媒体4の構成>

第一可搬媒体4は、例えば、DVD-ROMやCD-ROM等のようなあらかじめ動画データなどが暗号化されて書き込まれている可搬媒体であり、図2に示すように、タイトル識別子TLIDと、タイトル識別子TLIDに対応するタイトル鍵TLKを基にコンテンツCNTが暗号化された暗号化コンテンツENCNT=Enc(TLK, CNT)が記録されている。なお、Enc(K, P)を平文Pを暗号化鍵Kで暗号化した際の暗号文とし、以後同じ表記を用いる。タイトル識別子TLIDは、第一可搬媒体4に蓄積されているコンテンツCNTの内容を一意に特定可能な識別子であり、コンテンツCNTは、利用者端末6a～6nにおいて外部へ出力可能なフォーマット形式のコンテンツデータである。例えば、タイトル識別子TLIDは、コンテンツCNTの映画や曲のタイトル、シリアル番号(1、2、3、...)などであって、コンテンツCNTは、MPEG2(Moving Picture Expert Group)フォーマットによる動画コンテンツデータなどである。

#### 【0016】

##### <第二可搬媒体5aの構成>

第二可搬媒体5aは、例えば、SDカード等のようにデータの読み書きが可能なポータブルメディアであり、以前に第二可搬媒体5aが挿入されたことのある利用者端末に関する端末情報と、その利用者端末向けの鍵情報であるタイトル識別子と暗号化タイトル鍵の組を保持出来るものである。図3では、利用者端末6aの端末情報と鍵情報を保持している状態を示している。なお、第二可搬媒体5aには複数の利用者端末の端末情報を保持しても良いし、一つの利用者端末用の鍵情報として、複数組のタイトル識別子と暗号化タイトル鍵を保持していても良い。暗号化タイトル鍵は、対応する利用者端末が保持する個別鍵を基にタイトル鍵TLKが暗号化された値である。端末情報は、利用者端末識別子と、利用者端末識別子に対応する第一利用者端末乱数と第二利用者端末乱数と、を含む。利用者端末識別子は、利用者端末6a～6nそれぞれを一意に特定可能な識別子である。第一利用者端末乱数は、第二可搬媒体5aが対応する利用者端末に最後に挿入された時点で利用者端末が保持していた乱数であり、第二利用者端末乱数は、利用者端末の保持する乱数を更新するために管理センタ2が書き込む乱数の値である。個別鍵IKa～IKnは、利用者端末6a～6nそれが保持する鍵であり、タイトル鍵TLKは第一可搬媒体4に記録されるコンテンツCNTを暗号化及び復号化する際に用いられる鍵であり、第一可搬媒体4に記録されるコンテンツタイトル毎に異なる鍵である。例えば、第一利用者端末乱数と第二利用者端末乱数と個別鍵とタイトル鍵は、128ビットの自然数である。なお、第二利用者端末乱数及び暗号化タイトル鍵は必ずしも記録されていなくてもよい。

## 【0017】

### <管理センタ2の構成>

管理センタ2は、図4に示すように、管理センタ送受信部21と管理センタ表示部22と管理センタ記録部23と管理センタ制御部24とから構成される。

#### (1) 管理センタ送受信部21

管理センタ送受信部21は、モ뎀等であって、通信路上の情報収集サーバ3からの送信データを受信したり、情報収集端末3へデータを送信したりする。管理センタ送受信部21は、通信プロトコルとして、たとえば、TCP/IPを用いる。

## 【0018】

#### (2) 管理センタ表示部22

管理センタ表示部22は、液晶パネルやディスプレイ等であって、管理センタ制御部24からの指示に応じて、必要な画面を表示する。

#### (3) 管理センタ記録部23

管理センタ記録部23は、図5に示すように、予め与えられる利用者端末6a～6nの端末情報である利用者端末識別子TMI Da～TMI Dnと第一管理センタ乱数CRND1a～CRND1nと個別鍵IKa～IKn、及び、予め与えられるタイトル鍵情報であるタイトル識別子とタイトル鍵TLKの組を一組以上記録されている。また、各利用者端末識別子TMI Da～TMI Dnに対応して、第二管理センタ乱数CRND2a～CRND2nも記録可能である。第一管理センタ乱数は、第二可搬媒体から端末情報を受け取った最後の時点で対応する利用者端末が保持していた乱数であり、第二管理センタ乱数は、利用者端末の保持する乱数を更新するために管理センタ2が以前第二可搬媒体に書き込んだ乱数の値である。なお、第一管理センタ乱数CRND1a～CRND1nと第二管理センタ乱数CRND2a～CRND2nの値は変更可能である。例えば、第一管理センタ乱数と第二管理センタ乱数は、128ビットの自然数である。なお、第二利用者端末乱数は必ずしも記録されていなくてもよい。

## 【0019】

#### (4) 管理センタ制御部24

管理センタ制御部24は、図4で示すとおり、管理センタ受信処理部241と、端末情報確認部242と、端末情報生成部243と、タイトル鍵暗号化部244と、管理センタ送信データ生成部245と、管理センタ送信処理部246とを含む。管理センタ制御部24は、各機能部を有する専用のマイクロコンピュータ等である。各機能部は、マイクロコンピュータにマスクされているプログラムによって実現される。なお、各機能部は、独立のマイクロコンピュータであってもよい。

## 【0020】

#### (4-1) 管理センタ受信処理部241

管理センタ受信処理部241は、管理センタ送受信部21を介して、情報収集サーバ3から利用者端末識別子と第一利用者端末乱数とタイトル識別子を受け取る。そして、受け取った利用者端末識別子と第一利用者端末乱数を端末情報確認部242へ出力し、利用者端末識別子とタイトル識別子をタイトル鍵暗号化部244へ出力する。

## 【0021】

#### (4-2) 端末情報確認部242

端末情報確認部242は、管理センタ受信処理部241から利用者端末識別子と第一利用者端末乱数を取得する。そして、管理センタ記録部23から、受け取った利用者端末識別子に対応する第一管理センタ乱数を取得する。また、利用者端末識別子に対応する第二管理センタ乱数が記録されている場合、第二管理センタ乱数も取得する。

## 【0022】

まず、第二管理センタ乱数が記録されている場合、第一利用者端末乱数と第二管理センタ乱数が一致しているかどうか確認する。そこで、第一利用者端末乱数と第二管理センタ乱数が一致している場合、管理センタ記録部23に記録されている第一管理センタ乱数の値に第二管理センタ乱数の値をコピーし、第二管理センタ乱数を消去する。そして、端末

情報生成部243へ利用者端末識別子を出力し、タイトル鍵暗号化部244へ暗号化タイトル鍵生成要求を出力する。次に、第二管理センタ乱数が記録されているが第一利用者端末乱数と第二管理センタ乱数が一致しない場合、もしくは、第二管理センタ乱数が記録されていない場合、第一利用者端末乱数と第一管理センタ乱数が一致しているかどうか確認する。そこで、第一利用者端末乱数と第一管理センタ乱数が一致していない場合、利用者端末識別子に対応する利用者端末がクローンであることを示す画面を管理センタ表示部22に表示させる。一方、第一利用者端末乱数と第一管理センタ乱数が一致していた場合、端末情報生成部243へ利用者端末識別子を出力し、タイトル鍵暗号化部244へ暗号化タイトル鍵生成要求を出力する。

#### 【0023】

##### (4-3) 端末情報生成部243

端末情報生成部243は、端末情報確認部242から利用者端末識別子を取得する。そこでまず乱数を生成する。乱数を生成する方法については公知であるので説明を省略する。そして、その乱数を、管理センタ記録部23の利用者端末識別子に対応する第二管理センタ乱数として記録する。また、同一の乱数を、第二利用者端末乱数として、管理センタ送信データ生成部245へ出力する。

#### 【0024】

##### (4-4) タイトル鍵暗号化部244

タイトル鍵暗号化部244は、管理センタ受信処理部241から利用者端末識別子とタイトル識別子を取得する。また、端末情報確認部242から暗号化タイトル鍵生成要求を取得する。そして、まず、管理センタ記録部23から、利用者端末識別子に対応する個別鍵を取得する。また、タイトル識別子に対応するタイトル鍵を取得する。その後、個別鍵を基にタイトル鍵を暗号化して、暗号化タイトル鍵を生成する。最後に、タイトル識別子と暗号化タイトル鍵を管理センタ送信データ生成部245へ出力する。

#### 【0025】

##### (4-5) 管理センタ管理センタ送信データ生成部245

管理センタ送信データ生成部245は、端末情報生成部243から第二利用者端末乱数を取得する。また、タイトル鍵暗号化部244からタイトル識別子と暗号化タイトル鍵を取得する。そして、取得した第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵から、情報収集サーバ3へ送付するデータを生成する。そして、その生成したデータを管理センタ送信処理部246に出力する。

#### 【0026】

##### (4-6) 管理センタ管理センタ送信処理部246

管理センタ送信処理部246は、管理センタ送信データ生成部245からデータを取得する。そして、そのデータを管理センタ送受信部21を介して、情報収集サーバ3へ送信する。

#### <管理センタ2の動作>

以上で、管理センタ2の構成について説明を行ったが、次に管理センタ2の動作についてフローチャートを用いて説明する。ここでは、情報収集サーバ3から利用者端末識別子T M I D aと第一利用者端末乱数T M R N D 1 aとタイトル識別子T L I Dを受け取った場合を例に挙げ、図6を用いて説明する。

#### 【0027】

管理センタ受信処理部241は、情報収集サーバ3から利用者端末識別子T M I D aと第一利用者端末乱数T M R N D 1 aとタイトル識別子T L I Dを受け取り、その利用者端末識別子T M I D aと第一利用者端末乱数T M R N D 1 aとを端末情報確認部242へ出力し、利用者端末識別子T M I D aとタイトル識別子T L I Dをタイトル鍵暗号化部244へ出力する。(S201)

端末情報確認部242は、管理センタ受信処理部241から利用者端末識別子T M I D aと第一利用者端末乱数T M R N D 1 aを取得する。(S202)

管理センタ記録部23に利用者端末識別子T M I D aに対応する第二管理センタ乱数C

R N D 2 a が記録されている場合、ステップ S 2 0 4 に進む。一方、利用者端末識別子 T M I D a に対応する第二管理センタ乱数 C R N D 2 a が記録されていない場合、ステップ S 2 0 7 に進む。(S 2 0 3)

端末情報確認部 2 4 2 は、管理センタ記録部 2 3 から第二管理センタ乱数 C R N D 2 a を取得する。(S 2 0 4)

第一利用者端末乱数 T M R N D 1 a の値と第二管理センタ乱数 C R N D 2 a の値が一致している場合、ステップ S 2 0 6 に進む。一方、第一利用者端末乱数 T M R N D 1 a の値と第二管理センタ乱数 C R N D 2 a の値が一致していない場合、ステップ S 2 0 7 に進む。(S 2 0 5)

第一管理センタ乱数 C R N D 1 a の値に第二管理センタ乱数 C R N D 2 a の値をコピーし、第二管理センタ乱数 C R N D 2 a を消去する。ステップ S 2 1 0 に進む。(S 2 0 6)

端末情報確認部 2 4 2 は、管理センタ記録部 2 3 から、その利用者端末識別子 T M I D a に対応する第一管理センタ乱数 C R N D 1 a を取得する。(S 2 0 7)

第一利用者端末乱数 T M R N D 1 a の値と第一管理センタ乱数 C R N D 1 a の値が一致している場合、ステップ S 2 1 0 に進む。一方、第一利用者端末乱数 T M R N D 1 a の値と第一管理センタ乱数 C R N D 1 a の値が一致していない場合、ステップ S 2 0 9 に進む。(S 2 0 8)

端末情報確認部 2 4 2 は、利用者端末識別子 T M I D a に対応する利用者端末がクローンであることを示す画面を管理センタ表示部 2 2 に表示させ、ステップ S 2 1 0 へ進む。例えば、「クローンを見つかりました：利用者端末識別子 T M I D a」と表示する。ステップ S 2 1 0 へ進む。(S 2 0 9)

端末情報確認部 2 4 2 は、端末情報生成部 2 4 3 へ利用者端末識別子 T M I D a を出力し、タイトル鍵暗号化部 2 4 4 へ暗号化タイトル鍵生成要求を出力する。(S 2 1 0)

端末情報生成部 2 4 3 は、端末情報確認部 2 4 2 から利用者端末識別子 T M I D a を取得する。そして、まず乱数を生成する。その乱数を管理センタ記録部 2 3 の利用者端末識別子 T M I D a に対応する第二管理センタ乱数 C R N D 2 a の値として記録する。また、同じ乱数を、第二利用者端末乱数 T M R N D 2 a として、管理センタ送信データ生成部 2 4 5 へ出力する。(S 2 1 1)

タイトル鍵暗号化部 2 4 4 は、管理センタ受信処理部 2 4 1 から利用者端末識別子 T M I D a とタイトル識別子 T L I D を取得する。また、端末情報確認部 2 4 2 から暗号化タイトル鍵生成要求を取得する。そこでまず、管理センタ記録部 2 3 から、利用者端末識別子 T M I D a に対応する個別鍵 I K a を取得する。また、タイトル識別子 T L I D に対応するタイトル鍵 T L K を取得する。そして、個別鍵 I K a を基にタイトル鍵 T L K を暗号化して、暗号化タイトル鍵 E N C T L K a = E n c ( T K , I K a ) を生成する。そして、タイトル識別子 T L I D と暗号化タイトル鍵 E N C T L K a を管理センタ送信データ生成部 2 4 5 へ出力する。(S 2 1 2)

管理センタ送信データ生成部 2 4 5 は、端末情報生成部 2 4 3 から第二利用者端末乱数 T M R N D 2 a を取得する。また、タイトル鍵暗号化部 2 4 4 からタイトル識別子 T L I D と暗号化タイトル鍵 E N C T L K a を取得する。そして、取得した第二利用者端末乱数 T M R N D 2 a とタイトル識別子 T L I D と暗号化タイトル鍵 E N C T L K a を情報収集サーバ 3 へ送付する送信データを生成する。そして、その生成した送信データを管理センタ送信処理部 2 4 6 に出力する。(S 2 1 3)

管理センタ送信処理部 2 4 6 は、管理センタ送信データ生成部 2 4 5 から送信データを取得する。そして、その送信データを管理センタ送受信部 2 1 を介して、情報収集サーバ 3 へ送信する。終了する。(S 2 1 4)

以上が、クローン端末発見システム 1 の構成要素である管理センタ 2 の構成と動作である。続いて、情報収集サーバ 3 の構成と動作について説明を行う。

【0028】

<情報収集サーバ 3 の構成>

情報収集サーバ3は、図7に示すように、情報収集サーバ送受信部31と可搬媒体アクセス部32と外部入力部33と情報収集サーバ制御部34とから構成される。

(1) 情報収集サーバ送受信部31

情報収集サーバ送受信部31は、モデム等であって、通信路上の管理センタ2からの情報を受信したり、管理センタ2へ情報を送信したりする。情報収集サーバ送受信部31は、通信プロトコルとして、たとえば、TCP/IPを用いる。

【0029】

(2) 情報収集サーバ第二可搬媒体アクセス部32

情報収集サーバ第二可搬媒体アクセス部32は、例えばSDカードリーダであって、情報収集サーバ3に第二可搬媒体が挿入されたことを検知したり、挿入されている第二可搬媒体に記録されているデータを取得したり、挿入されている第二可搬媒体にデータを記録したりする。

【0030】

(3) 外部入力部33

外部入力部33は、外部からタイトル識別子TLDを入力可能なものであって、例えば数字0～9やアルファベットA～Zを入力可能なキーボードやキーパッド、マウスである。

(4) 情報収集サーバ制御部34

情報収集サーバ制御部34は、情報収集サーバ第二可搬媒体挿入処理部341と、タイトル情報取得部342と、送信データ処理部343と、情報収集サーバ送信処理部344と、情報収集サーバ受信処理部345と、第二可搬媒体データ書込部346とを含む。情報収集サーバ制御部34は、各機能部を有する専用のマイクロコンピュータ等である。各機能部は、マイクロコンピュータにマスクされているプログラムによって実現される。なお、各機能部は、独立のマイクロコンピュータであってもよい。

【0031】

(4-1) 情報収集サーバ第二可搬媒体挿入処理部341

情報収集サーバ第二可搬媒体挿入処理部341は、情報収集サーバ第二可搬媒体アクセス部32経由で情報収集サーバ3に第二可搬媒体が挿入されたことを検知した場合、情報収集サーバ第二可搬媒体アクセス部32を介して第二可搬媒体に記録されている利用者端末識別子と第一利用者端末乱数を取得する。そして、受け取った利用者端末識別子と第一利用者端末乱数を情報収集サーバ送信データ生成部343へ出力し、タイトル情報要求をタイトル情報取得部342へ出力する。

【0032】

(4-2) タイトル情報取得部342

タイトル情報取得部342は、情報収集サーバ第二可搬媒体挿入処理部341からタイトル情報要求を受け取った場合、外部入力部33経由で、タイトル識別子を取得する。そして、取得したタイトル識別子を情報収集サーバ送信データ生成部343へ出力する。

(4-3) 情報収集サーバ送信データ生成部343

情報収集サーバ送信データ生成部343は、情報収集サーバ第二可搬媒体挿入処理部341から利用者端末識別子と第一利用者端末乱数を取得する。また、タイトル情報取得部342からタイトル識別子を取得する。そして、取得した利用者端末識別子と第一利用者端末乱数とタイトル識別子とから、管理センタ2へ送付する送信データを生成する。そして、その生成した送信データを情報収集サーバ送信処理部344に出力する。

【0033】

(4-4) 情報収集サーバ送信処理部344

情報収集サーバ送信処理部344は、情報収集サーバ送信データ生成部343から送信データを取得する。そして、その送信データを情報収集サーバ送受信部31を介して、管理センタ2へ送信する。

(4-5) 情報収集サーバ受信処理部345

情報収集サーバ受信処理部345は、情報収集サーバ送受信部31を介して、管理セン

タ2から第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵を受け取る。そして、受け取った第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵を第二可搬媒体データ書込部346へ出力する。

#### 【0034】

(4-6) 第二可搬媒体データ書込部346

第二可搬媒体データ書込部346は、情報収集サーバ受信処理部345から第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵を受け取る。そして、受け取った第二利用者端末乱数とタイトル識別子と暗号化タイトル鍵を情報収集サーバ第二可搬媒体アクセス部32経由で、第二可搬媒体へ記録する。

#### 【0035】

<情報収集サーバ3の動作>

以上で、情報収集サーバ3の構成について説明を行ったが、次に情報収集サーバ3の動作についてフローチャートを用いて説明する。ここでは、ユーザはタイトル識別子TLIDに対応するコンテンツの記録された第一可搬媒体4を購入し、ユーザが第二可搬媒体5aを保有しているとする。そして、情報収集サーバ3へその第二可搬媒体5aが挿入された場合を例に挙げ、図8を用いて情報収集サーバ3の動作を説明する。なお、情報収集サーバ3へ第二可搬媒体5aが挿入される前に、第二可搬媒体5aはそのユーザの保有する利用者端末6aへ挿入されていて、利用者端末6aの端末情報（利用者端末識別子TMI Daと第一利用者端末乱数TMRND1a）を取得しているとする。

#### 【0036】

情報収集サーバ第二可搬媒体挿入処理部341は、情報収集サーバ第二可搬媒体アクセス部32経由で情報収集サーバ3に第二可搬媒体5aが挿入されたことを検知する。（S301）

情報収集サーバ第二可搬媒体挿入処理部341は、情報収集サーバ第二可搬媒体アクセス部32を介して第二可搬媒体5aに記録されている利用者端末識別子TMI Daと第一利用者端末乱数TMRND1aを取得する。（S302）

情報収集サーバ第二可搬媒体挿入処理部341は、受け取った利用者端末識別子TMI Daと第一利用者端末乱数TMRND1aを情報収集サーバ送信データ生成部343へ出力し、タイトル情報要求をタイトル情報取得部342へ出力する。（S303）

タイトル情報取得部342は、情報収集サーバ第二可搬媒体挿入処理部341からタイトル情報要求を受け取り、外部入力部33経由で、タイトル識別子TLIDを取得する。（S304）

タイトル情報取得部342は、取得したタイトル識別子TLIDを情報収集サーバ送信データ生成部343へ出力する。（S305）

情報収集サーバ送信データ生成部343は、情報収集サーバ第二可搬媒体挿入処理部341から利用者端末識別子TMI Daと第一利用者端末乱数TMRND1aを取得し、タイトル情報取得部342からタイトル識別子TLIDを取得する。そして、取得した利用者端末識別子TMI Daと第一利用者端末乱数TMRND1aとタイトル識別子TLIDから、管理センタ2へ送付する送信データを生成する。そして、生成した送信データを情報収集サーバ送信処理部344に出力する。（S306）

情報収集サーバ送信処理部344は、情報収集サーバ送信データ生成部343から送信データを取得し、その送信データを情報収集サーバ送受信部31を介して、管理センタ2へ送信する。（S307）

情報収集サーバ受信処理部345は、通信路1を介して、管理センタ2から送信データを受信した場合、ステップS309へ進む。もし受信していない場合、ステップS308を繰り返す。（S308）

情報収集サーバ受信処理部345は、情報収集サーバ送受信部31を介して、管理センタ2から第二利用者端末乱数TMRND2aとタイトル識別子TLIDと暗号化タイトル鍵ENCTLKaを受け取る。そして、受け取った第二利用者端末乱数TMRND2aとタイトル識別子TLIDと暗号化タイトル鍵ENCTLKaを第二可搬媒体データ書込部

346へ出力する。(S309)

第二可搬媒体データ書込部346は、情報収集サーバ受信処理部345から第二利用者端末乱数TMRND2aとタイトル識別子TLIDと暗号化タイトル鍵ENCTLKaを受け取り、受け取った第二利用者端末乱数TMRND2aとタイトル識別子TLIDと暗号化タイトル鍵ENCTLKaを情報収集サーバ第二可搬媒体アクセス部32経由で、第二可搬媒体5aへ記録する。(S310)

以上が、クローン端末発見システム1の構成要素である情報収集サーバ3の構成と動作である。続いて、利用者端末6aの構成と動作について説明を行う。

#### 【0037】

##### <利用者端末6aの構成>

利用者端末6aは、図9に示すように、利用者端末第二可搬媒体アクセス部61、第一可搬媒体アクセス部62、出力部63、利用者端末記録部64、利用者端末制御部65とから構成される。

##### (1) 利用者端末第二可搬媒体アクセス部61

利用者端末第二可搬媒体アクセス部61は、例えばSDカードリーダであって、利用者端末6aに第二可搬媒体が挿入されたことを検知したり、挿入されている第二可搬媒体に記録されているデータを取得したり、挿入されている第二可搬媒体にデータを記録したりする。

#### 【0038】

##### (2) 第一可搬媒体アクセス部62

第一可搬媒体アクセス部62は、例えばDVDドライブであって、利用者端末6aに第一可搬媒体が挿入されたことを検知したり、挿入されている第一可搬媒体に記録されているデータを取得したりする。

##### (3) 出力部63

出力部63は、例えば外部の液晶ディスプレイやプラズマテレビ等と接続され、利用者端末制御部65から受け取ったデータを外部へ表示するものである。

#### 【0039】

##### (4) 利用者端末記録部64

利用者端末記録部64は、図10に示すように、予め与えられる利用者端末6aに関する端末情報である利用者端末識別子TMIDAと第一利用者端末乱数TMRND1aと個別鍵IKaとが記録されている。また、利用者端末記録部64には、タイトル鍵情報であるタイトル識別子とタイトル鍵の組を複数記録可能である。なお、第一利用者端末乱数TMRND1aの値は変更可能である。また、タイトル識別子とタイトル鍵の組を追記することが可能である。

#### 【0040】

##### (5) 利用者端末制御部65

利用者端末制御部65は、利用者端末第二可搬媒体挿入処理部651と、端末情報書込部652と、暗号化タイトル鍵復号化部653と、端末情報更新部654と、第一可搬媒体挿入処理部655と、デスクランブル処理部656とを含む。利用者端末制御部65は、各機能部を有する専用のマイクロコンピュータ等である。各機能部は、マイクロコンピュータにマスクされているプログラムによって実現される。なお、各機能部は、独立のマイクロコンピュータであってもよい。

#### 【0041】

##### (5-1) 利用者端末第二可搬媒体挿入処理部651

利用者端末第二可搬媒体挿入処理部651は、利用者端末第二可搬媒体アクセス部61経由で利用者端末6aに第二可搬媒体が挿入されたことを検知する。そしてまず、利用者端末記録部64に記録されている利用者端末識別子TMIDAを取得する。その次に、利用者端末第二可搬媒体アクセス部61経由で第二可搬媒体に利用者端末識別子TMIDAが記録されているかどうか確認する。ここで、もし第二可搬媒体に利用者端末識別子TMIDAが記録されていない場合、端末情報書込部652へ利用者端末識別子TMIDAを

出力する。一方、第二可搬媒体に利用者端末識別子T M I D aが記録されている場合、第二可搬媒体に利用者端末識別子T M I D aに対応する第二利用者端末乱数T M R N D 2 aとタイトル識別子T L I Dと暗号化タイトル鍵E N C T L K aが記録されているかどうか確認する。ここで、もし第二可搬媒体に利用者端末識別子T M I D aに対応する第二利用者端末乱数T M R N D 2 aと暗号化タイトル鍵E N C T L K aが記録されている場合、第二利用者端末乱数T M R N D 2 aを端末情報更新部6 5 4へ出力し、タイトル識別子T L I Dと暗号化タイトル鍵E N C T L K aを暗号化タイトル鍵復号化部6 5 3へ出力する。そして、第二利用者端末乱数T M R N D 2 aの値を第一利用者端末乱数T M R N D 1 aの値として、利用者端末識別子T M I D aに対応付けて第二可搬媒体に記録する。

#### 【0 0 4 2】

##### (5-2) 端末情報書込部6 5 2

端末情報書込部6 5 2は、利用者端末第二可搬媒体挿入処理部6 5 1から利用者端末識別子T M I D aを取得する。その後、利用者端末記録部6 4に記録されている第一利用者端末乱数を取得し、利用者端末識別子T M I D aと第一利用者端末乱数T M R N D 1 aを第二可搬媒体に記録する。

#### 【0 0 4 3】

##### (5-3) 暗号化タイトル鍵復号化部6 5 3

暗号化タイトル鍵復号化部6 5 3は、利用者端末第二可搬媒体挿入処理部6 5 1からタイトル識別子T L I Dと暗号化タイトル鍵E N C T L K aを取得する。そして、利用者端末記録部6 4から個別鍵I K aを取得する。その次に、個別鍵I K aを基に暗号化タイトル鍵E N C T L K aの復号化を行い、タイトル鍵T L Kを取得する。最後に、タイトル識別子T L I Dとそのタイトル鍵T L Kを利用者端末記録部6 4へ新たに記録する。

#### 【0 0 4 4】

##### (5-4) 端末情報更新部6 5 4

端末情報更新部6 5 4は、利用者端末第二可搬媒体挿入処理部6 5 1から第二利用者端末乱数T M R N D 2 aを取得する。そして、利用者端末記録部6 4に記録されている第一利用者端末乱数T M R N D 1 aの値を、第二利用者端末乱数T M R N D 2 aの値に変更する。

#### 【0 0 4 5】

##### (5-5) 第一可搬媒体挿入処理部6 5 5

第一可搬媒体挿入処理部6 5 5は、第一可搬媒体アクセス部6 2経由で利用者端末6 aに第一可搬媒体4が挿入されたことを検知する。そしてまず、第一可搬媒体アクセス部6 2経由で第一可搬媒体4に記録されているタイトル識別子T L I Dを取得する。そして、タイトル識別子T L I Dに対応するタイトル鍵T L Kが利用者端末記録部6 4に記録されているかどうか確認する。もしタイトル識別子T L I Dに対応するタイトル鍵T L Kが記録されている場合、利用者端末記録部6 4からタイトル鍵T L Kを取得し、デスクランブル処理部6 5 6へ出力する。

#### 【0 0 4 6】

##### (5-6) デスクランブル処理部6 5 6

デスクランブル処理部6 5 6は、第一可搬媒体挿入処理部6 5 5からタイトル鍵T L Kを取得する。その後、第一可搬媒体アクセス部6 2経由で第一可搬媒体4に記録されている暗号化コンテンツを逐次取得し、タイトル鍵T L Kを基に暗号化コンテンツを逐次でスクランブルを行い、出力部6 3経由で外部へ逐次出力する。

#### 【0 0 4 7】

##### <利用者端末6 aの動作>

以上で、利用者端末6 aの構成について説明を行ったが、次に利用者端末6 aの動作について説明する。まず、利用者端末6 aへ第二可搬媒体5 aを挿入した場合の動作について図1 1に示すフローチャートを用いて説明する。続いて、利用者端末6 aへ第一可搬媒体4を挿入した場合の動作について図1 2に示すフローチャートを用いて説明する。

#### 【0 0 4 8】

## <利用者端末6aへ第二可搬媒体5aを挿入した場合の動作>

利用者端末第二可搬媒体挿入処理部651は、利用者端末第二可搬媒体アクセス部61経由で利用者端末6aに第二可搬媒体5aが挿入されたことを検知する。そしてまず、利用者端末記録部64に記録されている利用者端末識別子TMI Daを取得する。(S601)

第二可搬媒体5aに利用者端末識別子TMI Daが記録されている場合、ステップS604に進む。一方、第二可搬媒体5aに利用者端末識別子TMI Daが記録されていない場合、ステップS603に進む。(S602)

端末情報書込部652へ利用者端末識別子TMI Daを出力する。端末情報書込部652は、利用者端末第二可搬媒体挿入処理部651から利用者端末識別子TMI Daを取得する。その後、利用者端末記録部64に記録されている第一利用者端末乱数を取得し、利用者端末識別子TMI Daと第一利用者端末乱数TMRND1aを第二可搬媒体5aに記録する。終了する。(S603)

第二可搬媒体5aに利用者端末識別子TMI Daに対応する第二利用者端末乱数TMRND2aが記録されている場合、ステップS605に進む。第二可搬媒体5aに利用者端末識別子TMI Daに対応する第二利用者端末乱数TMRND2aが記録されていない場合、ステップS606に進む。(S604)

第二利用者端末乱数TMRND2aを端末情報更新部654へ出力する。端末情報更新部654は、利用者端末第二可搬媒体挿入処理部651から第二利用者端末乱数TMRND2aを取得する。そして、利用者端末記録部64に記録されている第一利用者端末乱数TMRND1aの値を、第二利用者端末乱数TMRND2aの値に変更する。(S605)

第二可搬媒体5aに利用者端末識別子TMI Daに対応するタイトル識別子TLIDと暗号化タイトル鍵ENCTLKaが記録されている場合、ステップS607に進む。第二可搬媒体5aに利用者端末識別子TMI Daに対応するタイトル識別子TLIDと暗号化タイトル鍵ENCTLKaが記録されていない場合、終了する。(S606)

暗号化タイトル鍵復号化部653は、利用者端末第二可搬媒体挿入処理部651からタイトル識別子TLIDと暗号化タイトル鍵ENCTLKaを取得する。そして、利用者端末記録部64から個別鍵IKaを取得する。その次に、個別鍵IKaを基に暗号化タイトル鍵ENCTLKaの復号化を行い、タイトル鍵TLKを取得する。最後に、タイトル識別子TLIDとそのタイトル鍵TLKを利用者端末記録部64へ記録する。終了する。(S607)

## <利用者端末6aへ第一可搬媒体4を挿入した場合の動作>

第一可搬媒体挿入処理部655は、第一可搬媒体アクセス部62経由で利用者端末6aに第一可搬媒体4が挿入されたことを検知する。(S651)

第一可搬媒体挿入処理部655は、第一可搬媒体アクセス部62経由で第一可搬媒体4に記録されているタイトル識別子TLIDを取得する。(S652)

利用者端末記録部64にタイトル識別子TLIDに対応するタイトル鍵TLKが記録されている場合、ステップS654へ進む。利用者端末記録部64にタイトル識別子TLIDに対応するタイトル鍵TLKが記録されていない場合、処理を終了する。(S653)

利用者端末記録部64からタイトル鍵TLKを取得し、デスクランブル処理部656へ出力する。(S654)

デスクランブル処理部656は、第一可搬媒体挿入処理部655からタイトル鍵TLKを取得する。その後、第一可搬媒体アクセス部62経由で第一可搬媒体4に記録されている暗号化コンテンツを逐次取得し、タイトル鍵TLKを基に暗号化コンテンツを逐次デスクランブルを行い、出力部63経由で外部へ逐次出力する。全暗号化コンテンツのデスクランブルと外部出力が終了したら、処理を終了する。(S655)

以上が、クローン端末発見システム1の構成要素である利用者端末6aの構成と動作である。なお、利用者端末6aと他の利用者端末6b～6nとの相違点は、利用者端末記録部64において予めそれぞれ異なる利用者端末識別子TMI Db～TMI Dnと第一利用

者端末乱数TMRND1b～TMRND1nと個別鍵IKb～IKnを保持している点が異なる。

#### 【0049】

尚、利用者端末制御部の各機能ブロックは典型的には集積回路であるLSIとして実現されていてもよい。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

#### 【0050】

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)や、LSI内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

#### 【0051】

##### <実施形態1の効果>

ここでは、利用者端末の一つ（ここでは6aとする）が内部解析され、利用者端末6aの端末情報として利用者端末識別子TMIDaと個別鍵IKaと第一利用者端末乱数TMRND1aが外部へ漏洩した場合を例に挙げ、本発明の実施形態1の効果を説明する。まず、その利用者端末6aの端末情報が外部に漏洩した場合、その端末情報を保持する大量のクローン端末（ここではその一つを6xとする）が市場に出回る可能性がある。つまり、利用者端末6aとクローン端末6xは同じ端末情報（利用者端末識別子TMIDaと個別鍵IKaと第一利用者端末乱数TMRND1a）を保持していることとなる。ここでは、利用者端末6aの利用者（利用者aと呼ぶ）とクローン端末6xの利用者（利用者xと呼ぶ）は異なると想定し、また、利用者aと利用者xはそれぞれ異なる第二可搬媒体5aと5xを保持しているとする。まず一般的なシナリオとして、利用者端末6aの利用者aが小売店にコンテンツの入った第一可搬媒体4を購入しに行くとする。その場合、利用者aの保持する第二可搬媒体5aを小売店に設置されている情報収集サーバ3に挿入する。ここで、管理センタ2は、第二可搬媒体5aに、暗号化されたタイトル鍵に加え、利用者端末識別子TMIDaの利用者端末向けの新たな乱数として第二利用者端末乱数を書き込む。利用者aはその第二可搬媒体5aを利用者端末6aに挿入し、利用者端末6aが保持する第一利用者端末乱数の値を第二可搬媒体5aに記録されている第二利用者端末乱数の値に更新する。そして、続いて利用者aが別のコンテンツを購入する際に、同様に第二可搬媒体5aを小売店に設置されている情報収集サーバ3に挿入する。その際、第二可搬媒体5aには第一利用者端末乱数として新しい乱数の値が設定されている。それを受け取った管理センタ2は、利用者端末識別子TMIDaに対応する利用者端末（6a）の第一利用者端末乱数が更新されたことを知る。その後、クローン端末6xの利用者xがコンテンツを購入しに小売店に行くとする。その際、利用者xは、同様に第二可搬媒体5xを小売店に設置されている情報収集サーバ3に挿入する。その際、その利用者xが保持する第二可搬媒体5xには、利用者端末識別子TMIDaと、端末情報が漏洩した時点の古い第一利用者端末乱数が書き込まれている。よって、管理センタ2は、利用者端末識別子TMIDaに対応する利用者端末（6x）が、古い第一利用者端末乱数を保持していると認識する。しかし、管理センタ2は、利用者端末識別子TMIDaに対応する利用者端末（6a）の第一利用者端末乱数が新たな乱数に更新されたと認識している。その結果から、同じ利用者端末識別子TMIDaを保持する利用者端末が市場に二台以上存在すると判断する。そして、利用者端末識別子TMIDaに対応する利用者端末にクローンが存在する旨、警告を表示する。このようにして、本発明の実施形態1では、利用者端末のクローンが存在することを効率的に発見、検知することが出来る。

## 【0052】

また、クローン利用者端末の別の形として、利用者端末の一つ（ここでも6aとする）が内部解析され、利用者端末6aに関する端末情報（利用者端末識別子TMI Daと個別鍵IKa第一利用者端末乱数TMRND1a）が外部へ漏洩した場合に、クローン検知を逃れる目的で、その利用者端末識別子（TMI Da）を違う偽の値（ここではTMI Dyとする）にしてクローン端末6yに埋め込む不正が考えられる。しかし、本発明の実施形態1では、管理センタ2は購入した暗号化コンテンツのタイトル鍵を、受け取った利用者端末識別子に対応する個別鍵で暗号化した暗号化タイトル鍵を提供するようにした。それにより、偽の利用者端末識別子TMI Dyを管理センタ2に渡した場合、そのクローン端末6yが保持する個別鍵IKaでは、受け取る暗号化タイトル鍵を復号化出来ないこととなる。つまり、クローン端末6yでは購入したコンテンツの出力が出来ないこととなる。これは、漏洩した利用者端末識別子を違う偽の値にして管理センタ2へ提供しても意味がないことに繋がる。よって、本発明の実施形態1では、漏洩した利用者端末識別子を偽造することの抑止力として効果的である。

## 【0053】

### <実施形態1の変形例>

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

(1) 本実施形態1では、第二可搬媒体が情報収集サーバに挿入される毎に、管理センタ2は新たな乱数を生成し、それを第二利用者端末乱数として第二可搬媒体に記録するようにして、利用者端末の乱数を毎回更新するようになっていたが、これに限るものではない。例えば、ある一定期間（例えば一ヶ月）に一回のみ乱数を更新するようにしてもよい。また、外部から乱数更新要求信号を受けた時にのみ、乱数を更新するようにしてもよい。また、ある一定回数（例えば10回）コンテンツを購入する毎に、乱数を更新するようにしてもよい。これは、乱数を更新しない場合に、管理センタ2は新たな乱数を生成せず、第二利用者端末乱数を第二可搬媒体に記録しないようにすることで実現可能である。

## 【0054】

(2) 本実施形態1では、端末情報として乱数を用いていたが、該当端末を保持しない第三者ユーザによって推定できず、さらに、管理センタ2が把握可能な値であれさえすれば、乱数でなくてもよい。例えば、シリアル番号で0から一つずつカウントアップしていくてもよい。また、管理センタ2が情報収集サーバからデータを受け取った時刻に関する情報でも良い。また、情報収集サーバ3へ第二可搬媒体が挿入された時刻に関する情報でも良い。また、情報収集サーバ3へ第二可搬媒体が挿入された延べ回数でも良い。また、対応する利用者端末で以前に外部へ出力したコンテンツタイトルの履歴に関する情報であってもよい。また、それらの値のハッシュ値であっても良い。

## 【0055】

(3) 本実施形態1では、端末情報として乱数を用いていたが、該当端末を保持しない第三者ユーザによって推定できず、さらに、各利用者端末が自動で更新される値であれさえすれば、乱数でなくてもよい。例えば、利用者端末に第二可搬媒体が最後に挿入された時刻情報でも良い。また、利用者端末に第二可搬媒体が挿入された延べ回数でも良い。この場合、管理センタ2は特に端末情報を更新する必要がなくなる。これにより、管理センタ2の手間を軽減することが可能となる。

## 【0056】

(4) 本実施形態1では、ユーザは第二可搬媒体を一つずつ保持している場合を例に説明を行ったが、これに限られるものではない。たとえば、一人のユーザが二枚以上の第二可搬媒体を保持していても良い。このような場合に、同じ利用者端末識別子を複数の第二可搬媒体が保持し、管理センタ2は、同じ利用者端末識別子を複数の第二可搬媒体経由で受け取る場合が考えられる。その際に、管理センタ2は、その利用者端末識別子に対応する第二利用者端末乱数を、その内の一つの第二可搬媒体にのみ書き込んでも良いし、一つ

の利用者端末識別子に対応する同じ第二利用者端末乱数を、複数の第二可搬媒体に書き込むようにしても良い。前者の場合、第二利用者端末乱数を書き込まれた第二可搬媒体をユーザが紛失した場合に、利用者端末の乱数を更新できないという欠点がある。一方、後者の場合、第二利用者端末乱数を書き込まれた第二可搬媒体をユーザが紛失した場合にでも、別の第二可搬媒体を用いて利用者端末の乱数を更新できるという利点がある。後者を実現するために、第二可搬媒体に記録する端末情報として乱数更新完了フラグを追加してもよい。乱数更新完了フラグは、第二可搬媒体に記録されている第二利用者端末乱数の値に、該当する利用者端末の第一利用者端末乱数の値の更新が完了した場合に、第二可搬媒体に書き込むフラグである。このようなフラグを追加することによって、一つの利用者端末識別子に対応する同じ第二利用者端末乱数を、複数の第二可搬媒体に書き込むようにして、その複数の第二可搬媒体を介して端末情報が管理センタ2へ提供されたとしても、乱数更新完了フラグが記録されている場合にのみ利用者端末の乱数更新が完了したと認識することが出来る。

#### 【0057】

(5) 本実施形態1では、第二可搬媒体はSDカード等のポータブルメディアであったが、これに限るものではない。例えば、演算処理の可能なICカードでも良い。その場合、例えば、第二可搬媒体は、暗号処理等で利用者端末を認証してから端末情報やタイトル鍵情報を提供するようにしてもよい。これにより、より安全なシステムを構築することが出来る。また、変形例(4)の乱数更新完了フラグをICカード内で追加するようにしてもよい。これにより、不正な利用者端末が、第二可搬媒体に乱数更新完了フラグを立てないという不正を排除することが出来る。

#### 【0058】

(6) 本実施形態1では、管理センタ2は、第二可搬媒体経由で端末情報を収集する見返りにタイトル鍵情報を提供していたが、これに限るものはない。例えば、管理センタ2は、管理センタ2は、第二可搬媒体経由で端末情報を収集するだけで、特に情報を提供しなくともよい。また、管理センタ2は、第二可搬媒体経由で端末情報を収集する見返りに一定期間(例えば1ヶ月)有効なライセンスを利用者端末に提供し、そのライセンスがある一定期間毎に取得しないと、利用者端末が利用不可になるような仕組みを備えていてもよい。

#### 【0059】

(7) 本実施形態1では、クローンを発見する対象は、コンテンツを出力する利用者端末であったが、本技術はこれに限るものではない。例えば、第二可搬媒体(例:SDカード)でも良い。また、電車の定期券や回数券や乗車券、ICカード、クレジットカード、キャッシュカード、デビットカード、電子マネー、電子チケット、電子パスポート(電子旅券)、入出門管理カード、運転免許書、住民基本台帳カード、携帯電話、PDA、STB(セットトップボックス)、電子ブック、コンピュータ、ICタグ、コンピュータソフトウェア、オンラインゲームのライセンスなどでもよい。この場合、クローンを発見する対象に、乱数を保持させることとなる。これにより、コンテンツを出力する利用者端末以外でも、クローンを発見することが出来る。

#### 【0060】

(8) 本実施形態1では、暗号化方法は、秘密鍵暗号方式AESを利用していたが、これに限るものではない。例えば、別の秘密鍵暗号方式(例えはDES)でも良いし、公開鍵暗号(例えはRSA方式)でもよいし、別の暗号方式でもよい。

(9) 本実施形態1では、管理センタ2が、同一の利用者端末識別子に対応する異なる二種類の第一利用者端末乱数を受け取った場合に、その利用者端末識別子に対応する利用者端末はクローンであると判断していたが、これに限るものではない。例えば、同一の利用者端末識別子に対応するある閾値(例えは3)以上の異なる第一利用者端末乱数を受け取った場合に、その利用者端末識別子に対応する利用者端末はクローンであると判断してもよい。これにより、クローンの誤検知の確率を少なくすることが出来る。また、これは、同じ利用者端末識別子を複数の利用者端末が共有するようなシステムにも適用出来る。

例えば、利用者端末識別子が、機種毎に共通な場合である。この場合、閾値としては、同じ利用者端末識別子を有する利用者端末の数以上に設定するようとする。このようにすることで、同じ利用者端末識別子を複数の利用者端末が共有するようなシステムであっても、クローンを検知することが出来る。

#### 【0061】

(10) 本実施形態1では、第二可搬媒体5a～5mは13個であったが、これに限るものではない。例えば、12個以下でもよいし、14個以上であってもよい。また、利用者端末6a～6nは14台であったが、これに限るものではない。例えば、15台以上であっても良いし、13台以下であっても良い。また、情報収集サーバ3の数は、1台以上であれば何台でも良い。また、第一可搬媒体4の数も、1個以上であれば何個でも良い。タイトル識別子及びタイトル鍵の種類も、1種類以上であれば何種類でも良い。

#### 【0062】

(11) 本発明は、上記に示す方法であるとしてもよい。また、これらの方針をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

#### 【0063】

(12) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

#### 【産業上の利用可能性】

#### 【0064】

コンテンツを端末へ配布するシステムにおいて、端末のクローンが存在するか否か判断を行う必要が生じた場合に、特に有用である。

#### 【図面の簡単な説明】

#### 【0065】

【図1】本発明の実施の形態1におけるクローン端末発見システム1の概要図

【図2】本発明の実施の形態1における第一可搬媒体4の構成例を示す図

【図3】本発明の実施の形態1における第二可搬媒体5aの構成例を示す図

【図4】本発明の実施の形態1における管理センタ2の構成例を示す図

【図5】本発明の実施の形態1における管理センタ記録部23の構成例を示す図

【図6】本発明の実施の形態1における管理センタ2の動作の一例を示す図

【図7】本発明の実施の形態1における情報収集サーバ3の構成例を示す図

【図8】本発明の実施の形態1における情報収集サーバ3の動作の一例を示す図

【図9】本発明の実施の形態1における利用者端末6aの構成例を示す図

【図10】本発明の実施の形態1における利用者端末記録部64の構成例を示す図

【図11】本発明の実施の形態1における利用者端末6aにおいて第二可搬媒体5aを挿入した際の動作の一例を示す図

【図12】本発明の実施の形態1における利用者端末6aにおいて第一可搬媒体4を挿入した際の動作の一例を示す図

## 【符号の説明】

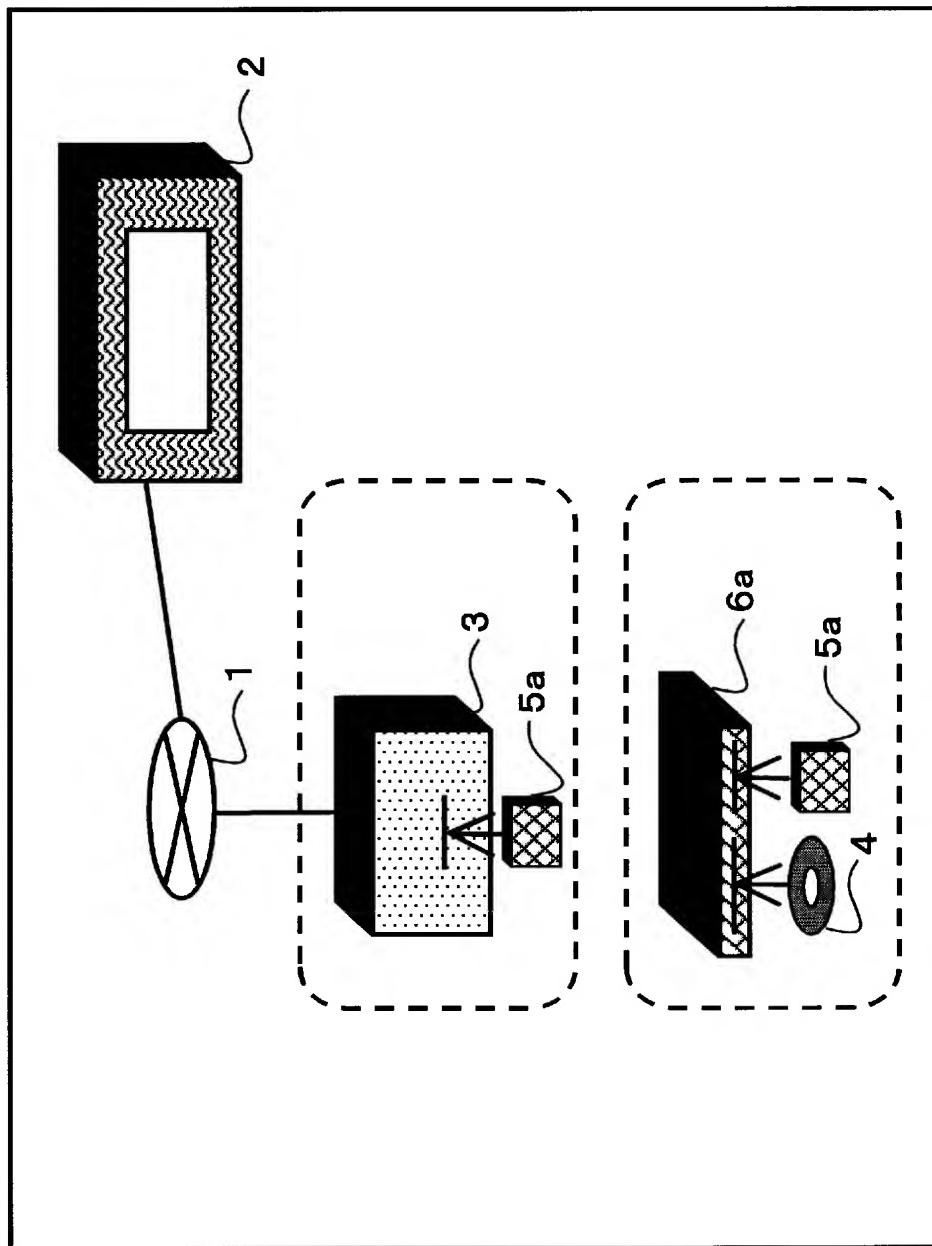
### 【0 0 6 6】

- 1 通信路
- 2 管理センタ
  - 2 1 管理センタ送受信部
  - 2 2 管理センタ表示部
  - 2 3 管理センタ記録部
  - 2 4 管理センタ制御部
    - 2 4 1 管理センタ受信処理部
    - 2 4 2 端末情報確認部
    - 2 4 3 端末情報生成部
    - 2 4 4 タイトル鍵暗号化部
    - 2 4 5 管理センタ送信データ生成部
    - 2 4 6 管理センタ送信処理部
  - 3 情報収集サーバ
    - 3 1 情報収集サーバ送受信部
    - 3 2 情報収集サーバ第二可搬媒体アクセス部
    - 3 3 外部入力部
    - 3 4 情報収集サーバ制御部
      - 3 4 1 情報収集サーバ第二可搬媒体挿入処理部
      - 3 4 2 タイトル情報取得部
      - 3 4 3 情報収集サーバ送信データ生成部
      - 3 4 4 情報収集サーバ送信処理部
      - 3 4 5 情報収集サーバ受信処理部
      - 3 4 6 第二可搬媒体データ書込部
  - 4 第一可搬媒体
    - 5 a～5 m 第二可搬媒体
    - 6 a～6 n 利用者端末
      - 6 1 利用者端末第二可搬媒体アクセス部
      - 6 2 第一可搬媒体アクセス部
      - 6 3 出力部
      - 6 4 利用者端末記録部
      - 6 5 利用者端末制御部
        - 6 5 1 利用者端末第二可搬媒体挿入処理部
        - 6 5 2 端末情報書込部
        - 6 5 3 暗号化タイトル鍵復号化部
        - 6 5 4 端末情報更新部
        - 6 5 5 第一可搬媒体挿入処理部
        - 6 5 6 デスクランブル部

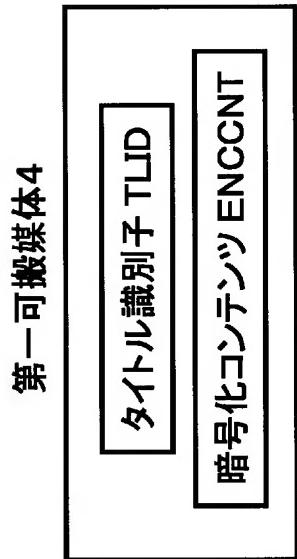
【書類名】 図面

【図 1】

クローン端末発見システム1

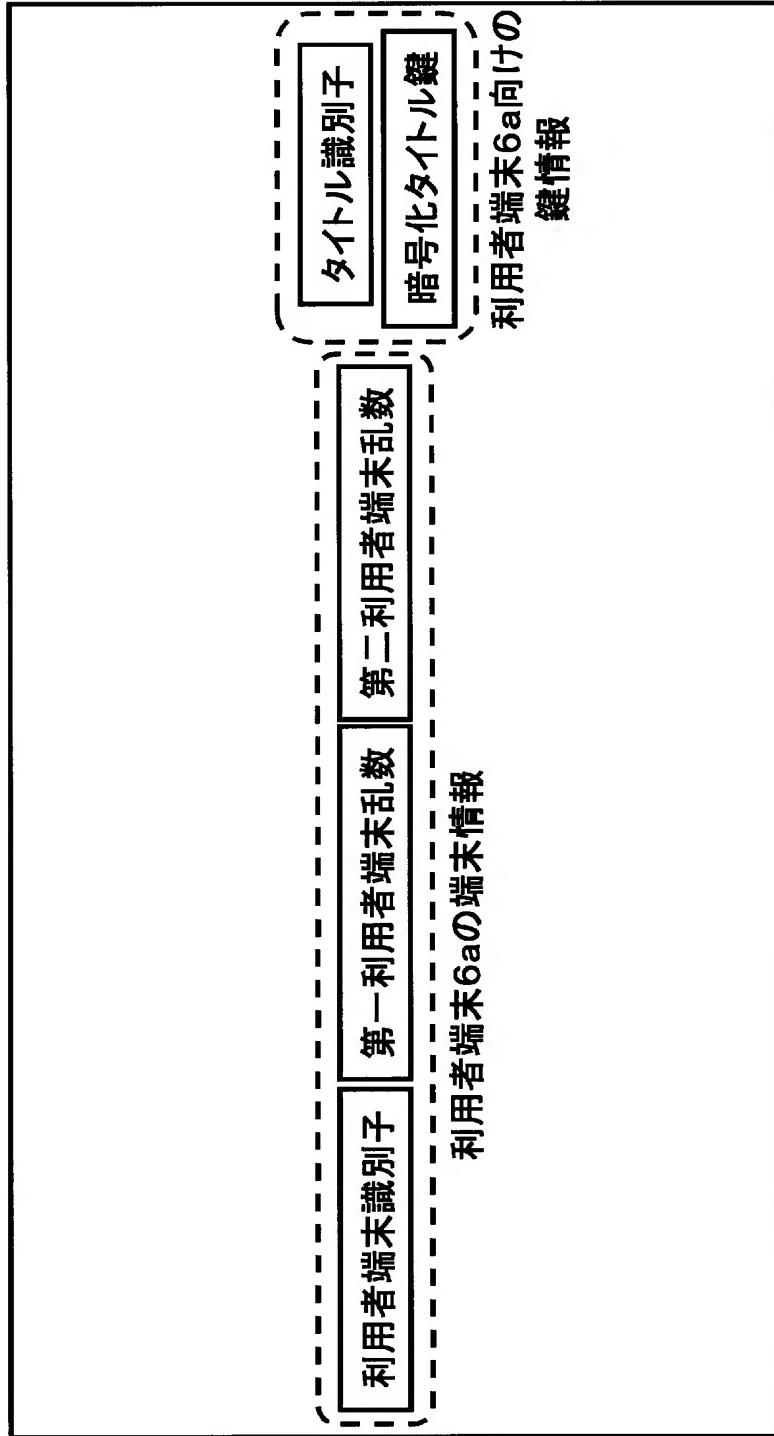


【図 2】

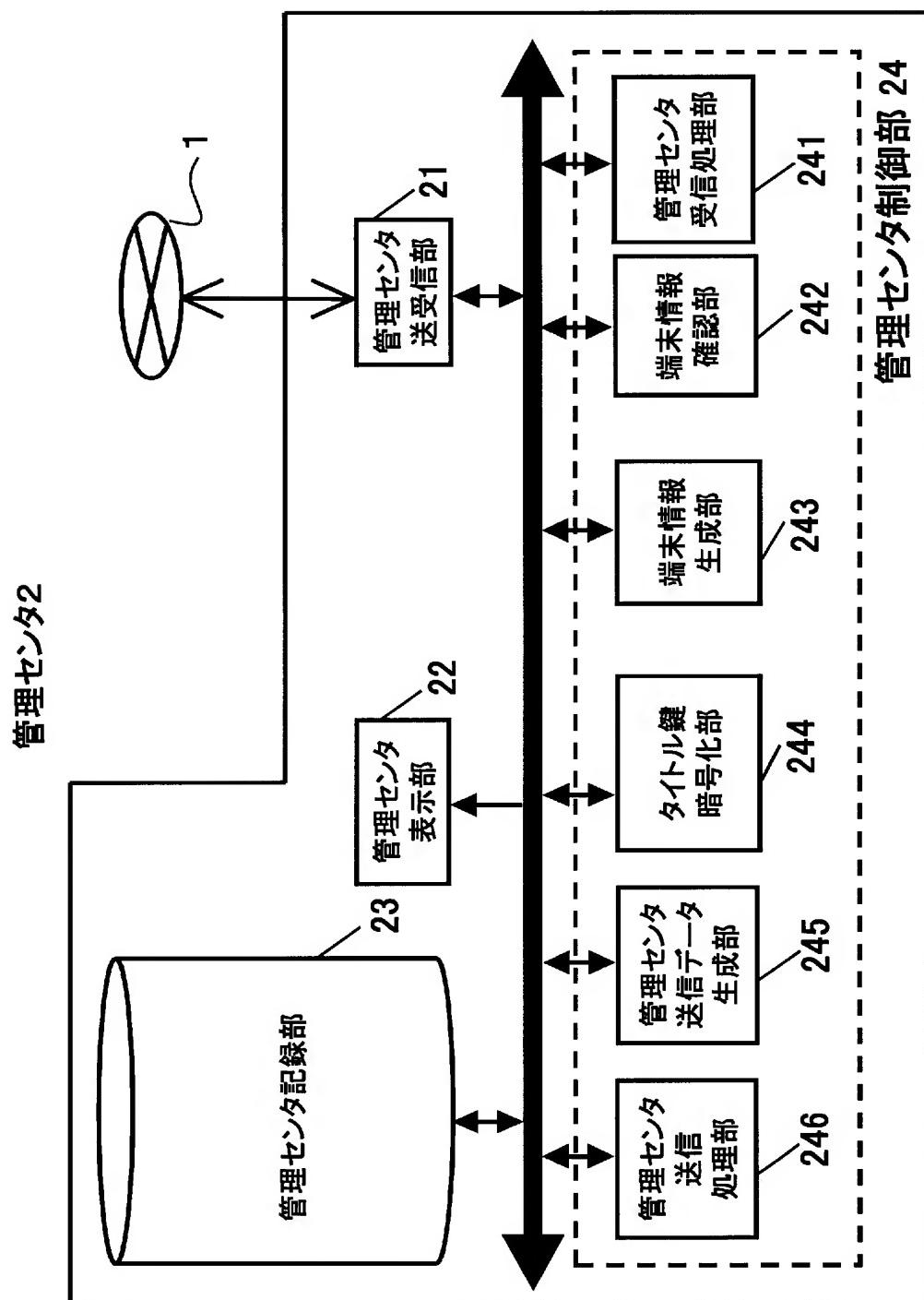


【図 3】

第二可搬媒体5a

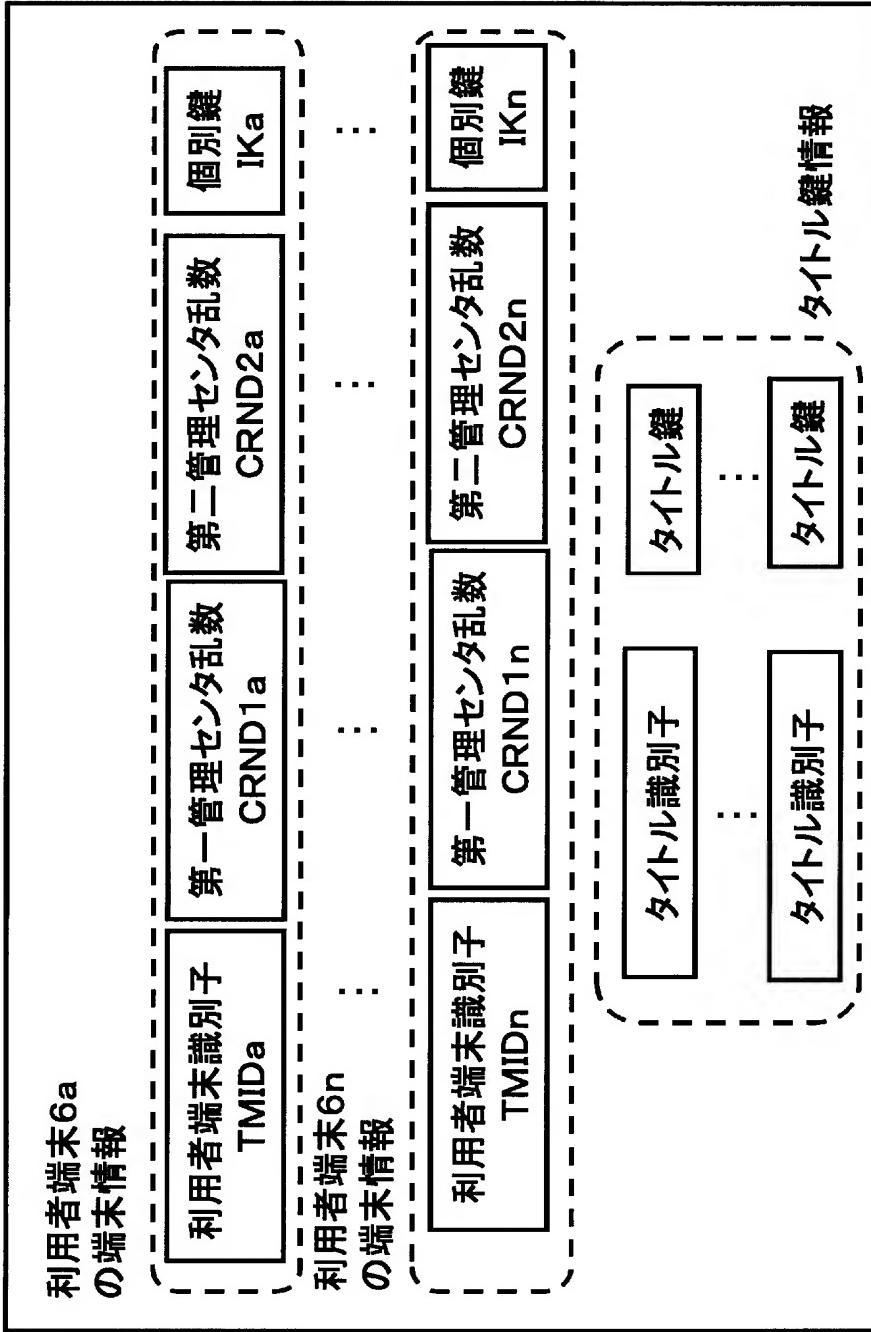


【図 4】

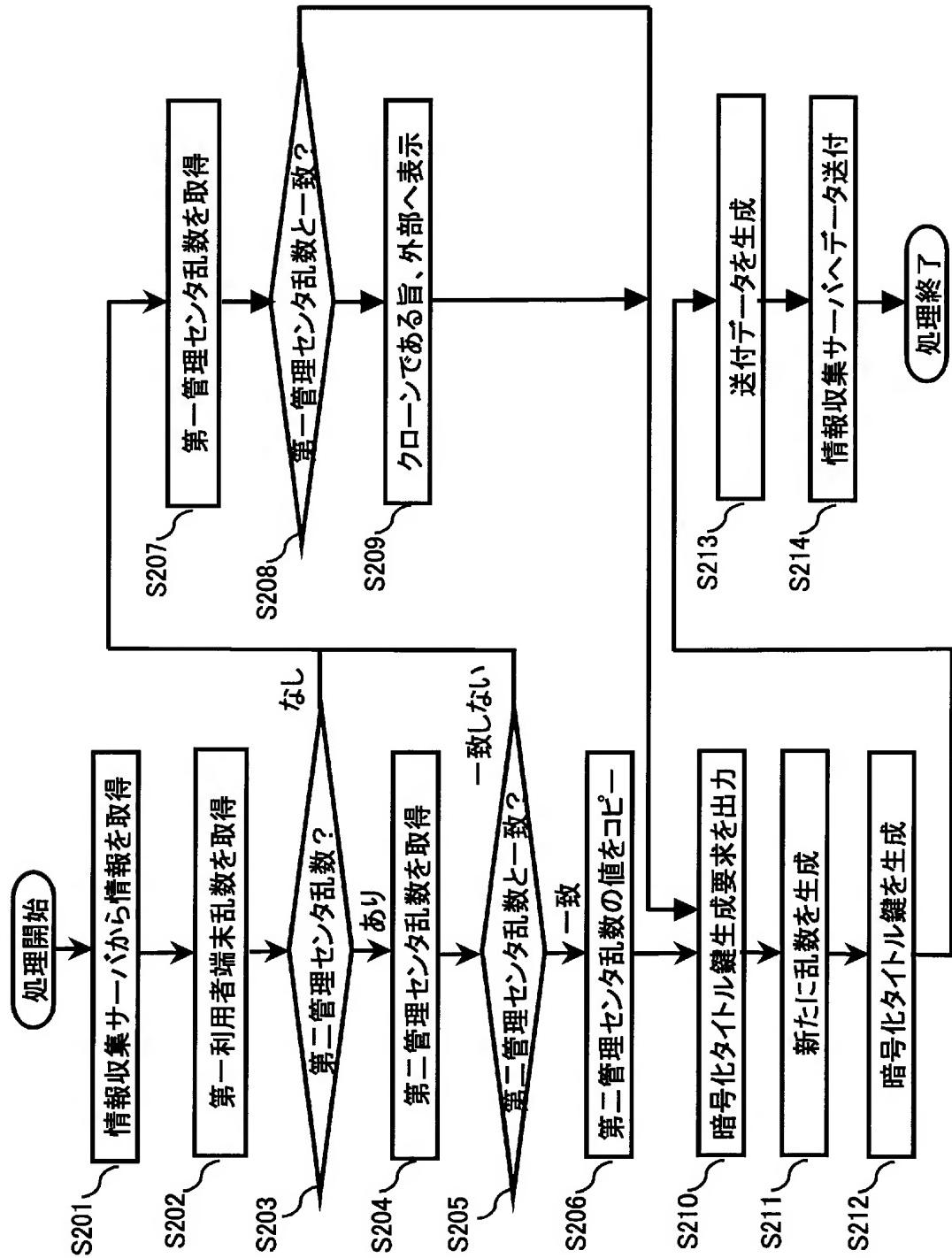


【図 5】

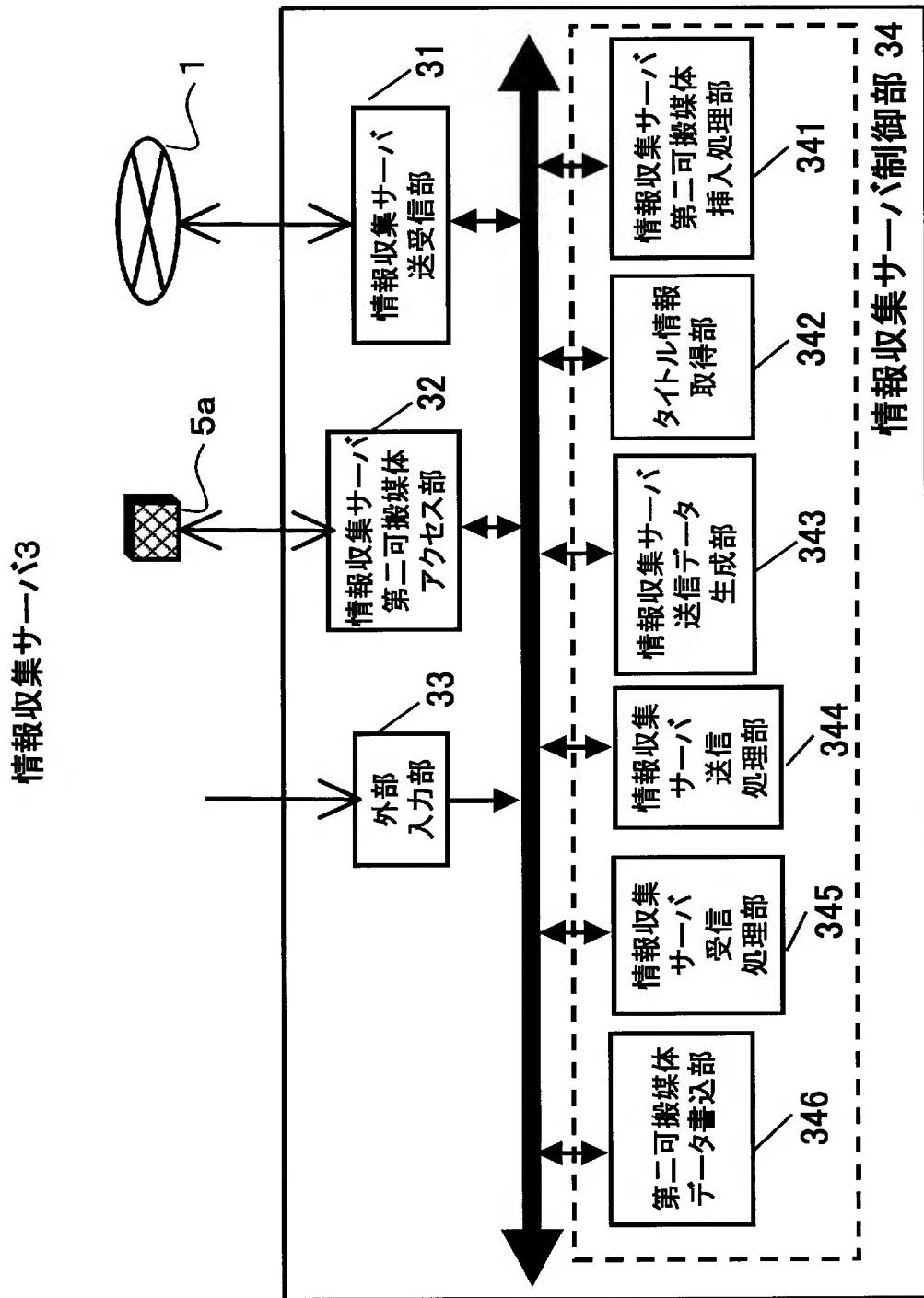
管理セシタ記録部23



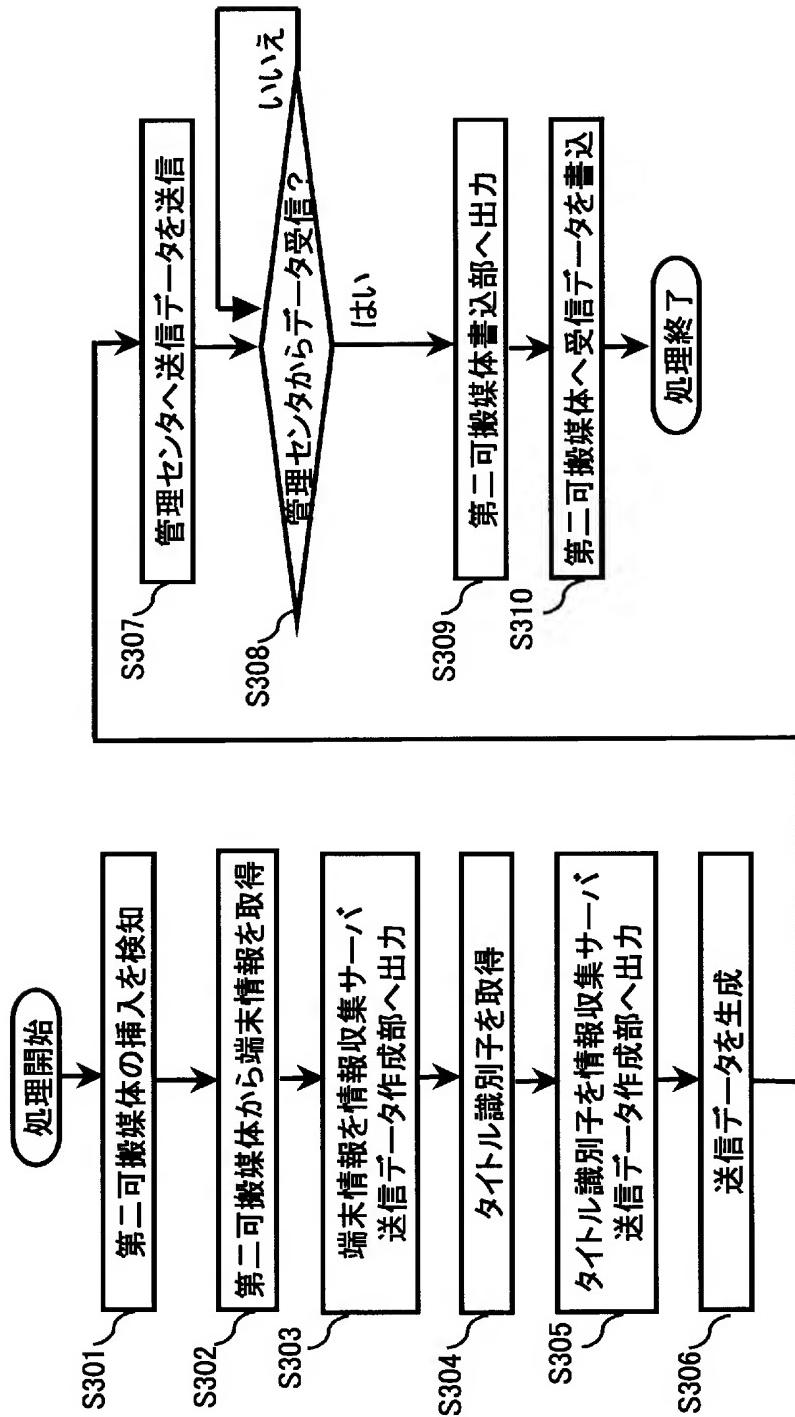
【図 6】



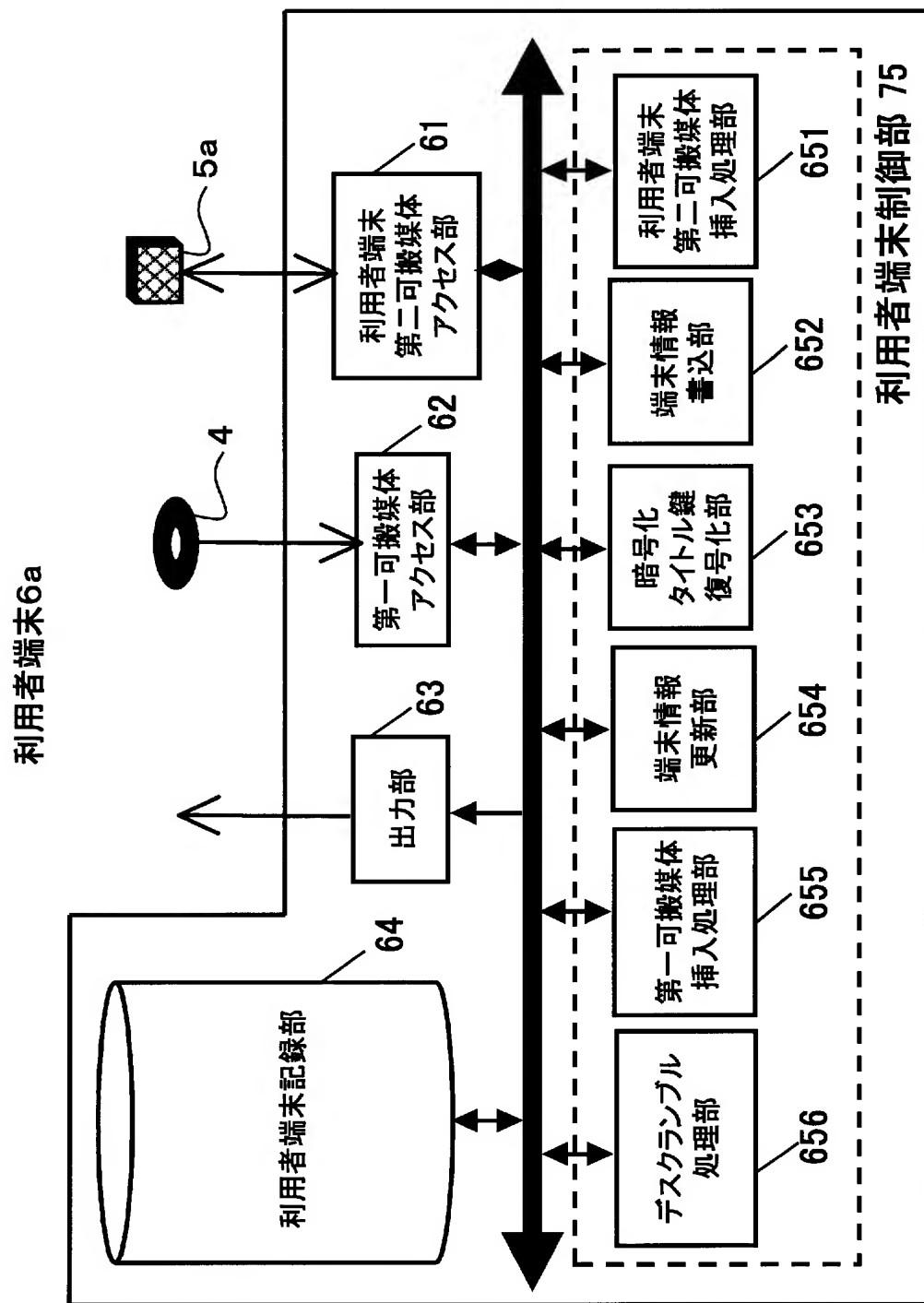
【図7】



【図 8】



【図 9】



【図 10】

利用者端末記録部64

利用者端末6aの端末情報

利用者端末識別子  
TMRNDa

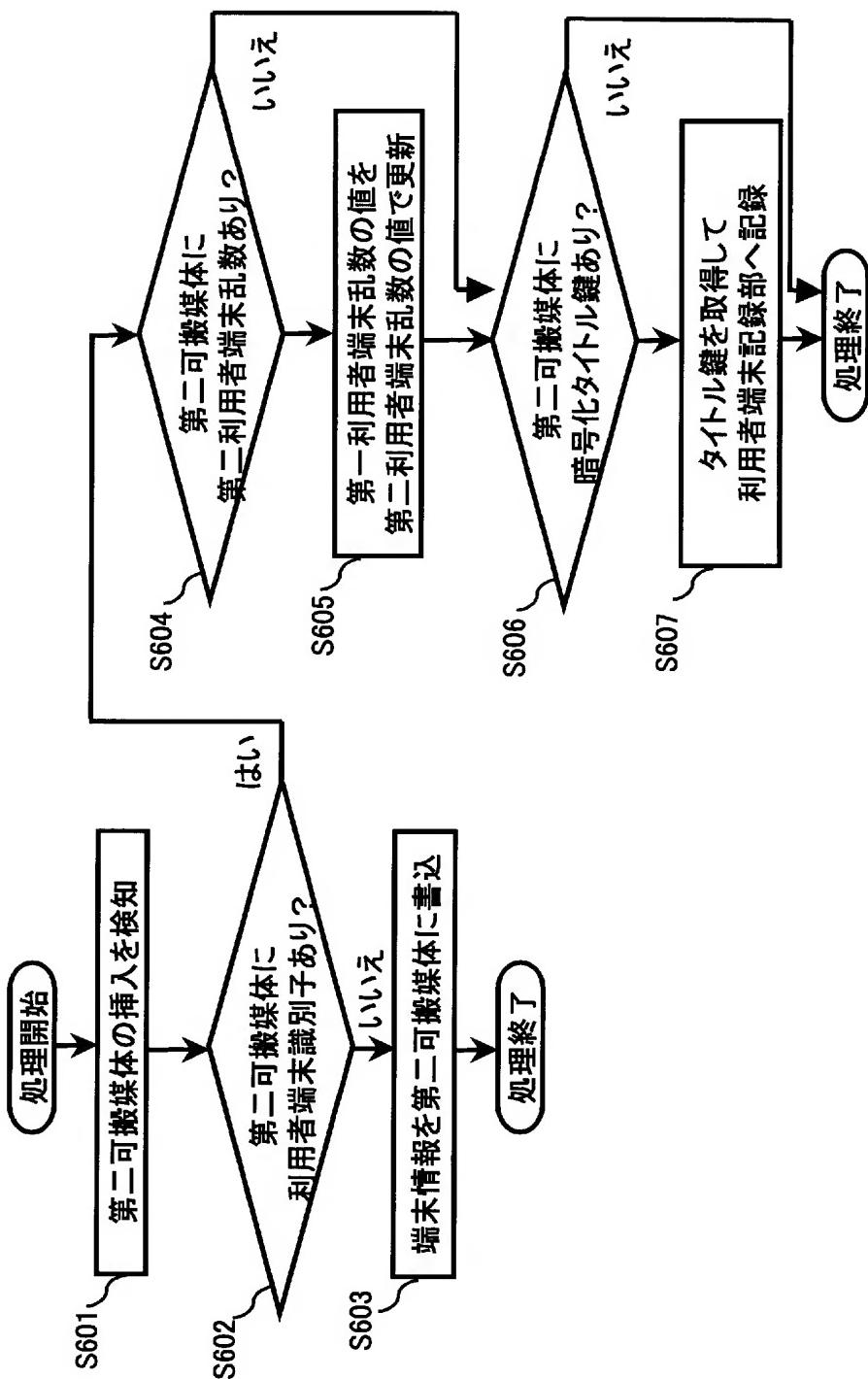
第一利用者端末乱数  
TMRND1a

個別鍵  
IKa

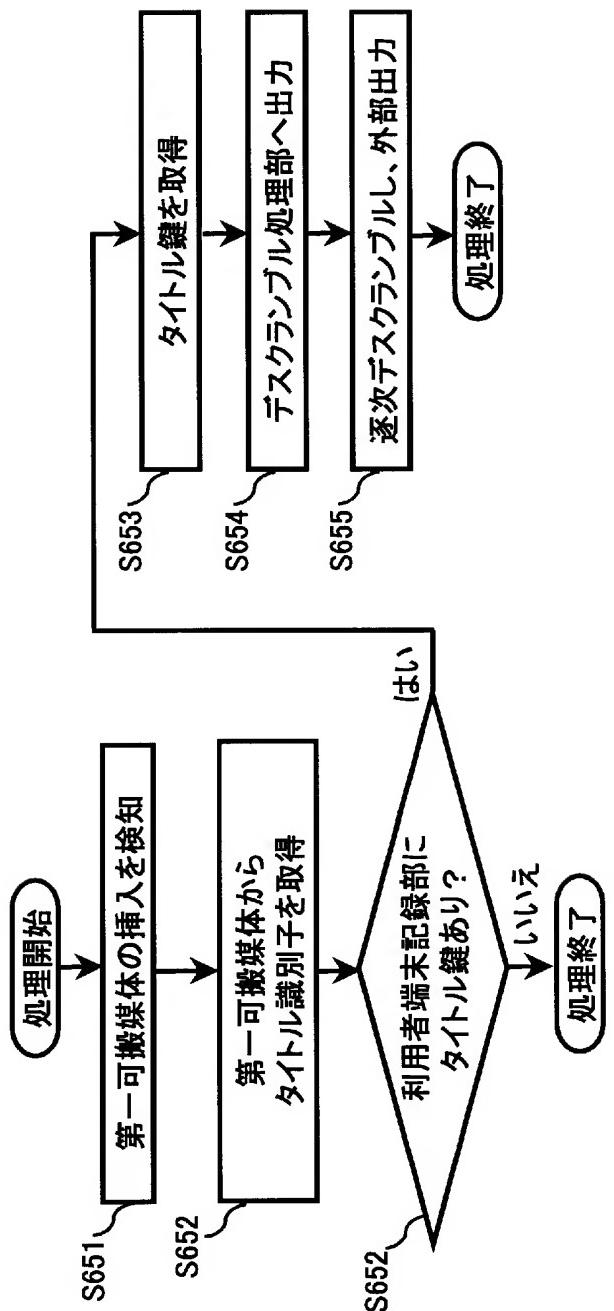
タイトル鍵  
：  
タイトル識別子  
：  
タイトル鍵  
：  
タイトル識別子  
：  
タイトル鍵  
：

タイトル鍵情報

【図 1-1】



【図 1-2】



【書類名】要約書

【要約】

【課題】外部に漏れた鍵を特定するためには、市場に大量流通したクローン端末／不正ソフトウェアを回収して、内部を解析することでしか特定できなかった

【解決手段】本発明は、利用者端末のクローンを発見するクローン端末発見システムであって、前記クローン端末発見システムは、前記利用者端末にクローンが存在するか否かを判断する管理センタと、前記利用者端末に関する利用者端末端末情報を前記管理センタへ供給する一以上の情報収集サーバと、前記利用者端末端末情報を前記情報収集サーバへ供給する一以上の前記利用者端末と、から構成され、前記管理センタと前記情報収集サーバは通信路を介して通信可能であって、前記管理センタは、管理センタ端末情報を保持する管理センタ記録手段と、前記情報収集サーバから前記利用者端末端末情報を取得する手段と、前記管理センタ端末情報を及び前記利用者端末端末情報を基に、前記利用者端末にクローンが存在するか否か判断する端末情報確認手段と、備え、前記情報収集サーバは、可搬媒体を介して、前記利用者端末から前記利用者端末端末情報を収集する情報収集サーバ可搬媒体挿入処理手段と、通信路を介して、前記前記利用者端末端末情報を前記管理センタへ供給する情報収集サーバ送信処理手段と、を備え、前記利用者端末は、前記利用者端末固有の前記利用者端末端末情報を保持する利用者端末記録手段と、前記可搬媒体を介して、前記利用者端末端末情報を前記情報収集サーバへ供給する可搬媒体データ書込手段と、を備えることを特徴とする。

【選択図】 図 1

【書類名】 手続補正書  
【整理番号】 2048160371  
【提出日】 平成17年 2月23日  
【あて先】 特許庁長官殿  
【事件の表示】  
  【出願番号】 特願2004-360436  
【補正をする者】  
  【識別番号】 000005821  
  【氏名又は名称】 松下電器産業株式会社  
【補正をする者】  
  【識別番号】 504137912  
  【氏名又は名称】 国立大学法人東京大学  
【代理人】  
  【識別番号】 100090446  
  【弁理士】  
  【氏名又は名称】 中島 司朗  
【発送番号】 005515  
【手数料補正】  
  【補正対象書類名】 特許願  
  【予納台帳番号】 014823  
  【納付金額】 16,000円

【書類名】 手続補正書  
【整理番号】 2048160371  
【提出日】 平成17年 3月30日  
【あて先】 特許庁長官 殿  
【事件の表示】  
  【出願番号】 特願2004-360436  
【補正をする者】  
  【識別番号】 000005821  
  【住所又は居所】 大阪府門真市大字門真1006番地  
  【氏名又は名称】 松下電器産業株式会社  
【補正をする者】  
  【識別番号】 504137912  
  【住所又は居所】 東京都文京区本郷7-3-1  
  【氏名又は名称】 国立大学法人東京大学  
【代理人】  
  【識別番号】 100090446  
  【住所又は居所】 大阪市北区豊崎3丁目2番1号淀川5番館6F  
  【弁理士】  
  【氏名又は名称】 中島 司朗  
【手続補正】  
  【補正対象書類名】 特許願  
  【補正対象項目名】 提出物件の目録  
  【補正方法】 追加  
  【補正の内容】  
    【提出物件の目録】  
    【物件名】 持分について証明する書面 1

【物件名】

持分について証明する書面

東大—松下電器連携契約準備

【添付書類】  
持分証明書



038

平成17年1月28日

事件の表示 平成16年12月13日付特許願 2004-360436号  
整理番号 (20481)H16-0371(乙内:依頼番号)  
3004Z014-1 (甲内:整理番号)

上記発明の特許を受ける権利の持分を国立大学法人 東京大学 50%、松下電器産業株式会社 50%と定めたことに相違ありません。

東京都文京区本郷七丁目三番一号

国立大学法人 東京大学

総長 佐々木 翁



大阪府門真市大字門真1006番地

松下電器産業株式会社

取締役社長 中村 邦夫



【書類名】 手続補正書  
【整理番号】 2048160371  
【提出日】 平成17年 8月 1日  
【あて先】 特許庁長官 殿  
【事件の表示】  
  【出願番号】 特願2004-360436  
【補正をする者】  
  【識別番号】 000005821  
  【住所又は居所】 大阪府門真市大字門真1006番地  
  【氏名又は名称】 松下電器産業株式会社  
【補正をする者】  
  【識別番号】 504137912  
  【住所又は居所】 東京都文京区本郷7-3-1  
  【氏名又は名称】 国立大学法人東京大学  
【代理人】  
  【識別番号】 100090446  
  【住所又は居所】 大阪市北区豊崎3丁目2番1号淀川5番館6F  
  【弁理士】 中島 司朗  
  【氏名又は名称】  
【発送番号】 052259  
【手続補正】  
  【補正対象書類名】 手続補正書  
  【補正対象書類提出日】 平成17年 3月 30日  
  【補正対象項目名】 持分について証明する書面  
  【補正方法】 変更  
  【補正の内容】  
    【提出物件の目録】  
    【物件名】 持分について証明する書面 1

【物件名】

持分について証明する書面

東大一松下電器連携契約準備

【添付書類】

持分証明書



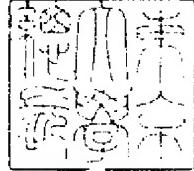
16 12 13  
平成 16 年 12 月 13 日

事件の表示 平成 16 年 12 月 13 日付特許願 2004-360436 号  
整理番号 (20481)H16-0371(乙内: 依頼番号)  
3004Z014-1 (甲内: 整理番号)

上記発明の特許を受ける権利の持分を国立大学法人 東京大学 50%、松下電器産業株式会社 50%と定めたことに相違ありません。

東京都文京区本郷七丁目三番一号

国立大学法人 東京大学  
総長 佐々木 翁



大阪府門真市大字門真 1006 番地

松下電器産業株式会社  
取締役社長 中村 邦夫



出願人履歴

000005821

19900828

新規登録

大阪府門真市大字門真1006番地

松下電器産業株式会社

504137912

20040406

新規登録

東京都文京区本郷7丁目3番1号

国立大学法人 東京大学